T1

BUSINESS CASE **'Doorontwikkeling IRU tot platform voor multidisciplinaire internet-aanpak'**	Versie: 0 3 Doc nummer:	
	Datum: 03-11-2017	
Naam opdrachtgever	GCT	Voor akkoord: Datum:
Naam opsteller	[redacted] (NP) [redacted] (Kmar) [redacted] (NCTV)	

10.2e

De bedragen in deze business case zijn schattingen op grond van de nu beschikbare kennis en feiten

Achtergrond

De manifestatie van jihadisten op (relatief) makkelijk toegankelijke plekken op het internet wordt door de inzet van overheden en marktpartijen teruggedrongen. [redacted]

10.2g & 10.2c

In 2017 is met het operationeel worden van de Internet Referral Unit bij de Nationale Politie een belangrijke stap gezet in de aanpak van online jihadisme. Datzelfde geldt voor het KMar OSINT team, wat zich richt op het monitoren, ondervangen en duiden van CT signalen in open bronnen incl. social media. [redacted]

10.2g & 10.2c

Tegelijkertijd wordt door verschillende organisaties met verschillende doeleinden en bevoegdheden in hetzelfde online jihadistische netwerk aan onderzoek, inlichtingenvergaring en/of content verwijdering gedaan. [redacted]

10.2g & 10.2c

Probleemstelling of ambitie

Bovenstaande ontwikkelingen maken het voor de operationele CT-partners noodzakelijk om zicht te houden/krijgen op de activiteiten van jihadisten online. [redacted] Daarom is het allereerst van belang om de IRU van de Nationale Politie te borgen en uit te bouwen, om vervolgens toe te werken naar een stevige multidisciplinaire internetaanpak met bijbehorende capaciteit in de vorm van een gezamenlijk platform (fte's, tooling, methodieken en opleidingen).

10.2g & 10.2c

Deze multidisciplinaire aanpak kan bestaan uit [redacted]

10.2g & 10.2c

De modus van deze multidisciplinaire aanpak wordt middels een haalbaarheidsstudie uitgewerkt. Op

basis van deze studie wordt vervolgens de verdere implementatie en uitvoering van deze aanpak vormgegeven. Omdat het wat betreft opleidingen en tooling gaat om innovatieve samenwerking, wordt ook budget geclaimd uit de innovatiegelden van ministerie JenV.

Beoogd doel
Borging en uitbouwen hoogwaardige capaciteit van de IRU en KMar en toewerken naar een stevig platform voor een multidisciplinaire internetaanpak. Hiertoe wordt voor mei 2018 een haalbaarheids-studie (eerste helft) uitgevoerd. Aan de hand van de uitkomsten daarvan wordt de multidisciplinaire aanpak geconcretiseerd.

10.2g & 10.2c

Toekomstige ontwikkelingen
[redacted]

Haalbaarheid en voorwaarden
Commitment van betrokken partijen (NP, Kmar, OM, AIVD, MIVD en NCTV) op uitvoeren haal-baarheidsstudie, borging IRU en toewerken naar platform voor multidisciplinaire internetaanpak.

Veranderingen & effecten op organisatie(s)
Bij de uitvoering van het beleidsvoornemen zullen waar nodig alle CT-partners (zoals politie, AIVD, OM, KMar, MIVD, DGPol, DGRR en NCTV (DAS, DCS en DCT) worden betrokken.

Duur en moment van het traject
Zie begroting

Kosten per jaar	**2018**	**2019**	**2020**	**2021 e.v.**
Onderzoekskosten	100.000	100.000	50.000	50.000
Borging en uit-bouw IRU	1.200.000	1.700.000	1.700.000	1.700.000
OSINT capaciteit KMar	250.000	250.000	250.000	250.000
Ontwikkel- en implementatie-kosten (o m tooling en oplei-ding)	650.000	800.000	800.000	300.000
Exploitatiekosten multidisplinaire aanpak (fte's, locatie etc)	500.000	1.100.000	1.200.000	1.200.000
Innovatiegeld JenV (aanvraag wordt voor eind 2017 ingediend)	*750 000*	*750 000*	*500 000*	*0*
Totaal CT gelden	**1.950.000€**	**3.500.000€**	**3.500.000€**	**3.500.000€**
Totaal Budget	**2.700.000€**	**4.250.000€**	**4.000.000€**	**3.500.000€**

Baten

[redacted]

10.2.g & 10.2c

Afgestemd met onderstaande partners

Het voorliggende voorstel wordt ondersteund door de volgende partners:

- NP
- KMar
- NCTV
- MIVD??
- DGPOL
- OM

10.2e

Met opmerkingen [JB1]: Maandag hierover contact met [redacted]

Met opmerkingen [JB2]: PM reactie [redacted], contact via NP

Met opmerkingen [JB3]: PM reactie [redacted] PAG



memo

Organisatieonderdeel Landelijke Eenheid
Dienst Landelijke Informatie
Voorziening (DLIO)
ALI

Aan DO

Behandeld door [redacted]
10.2e **Functie**
Telefoon
E-mail

Datum 22-09-2016
Bijlage(n) geen
Pagina 1

Onderwerp **Voortgang NTA**

Inleiding

Naar aanleiding van maatregel 29 uit het *Actieprogramma Integrale Aanpak Jihadisme*[1] heeft de politie de opdracht gekregen om de Nederlandse Internet Referral Unit (IRU) op te zetten. Kerntaak van deze unit is bestrijding van verspreiding van jihadpropaganda op openbare (sociale media) accounts op internet. Dit gebeurt via *Notice and Take Action* (NTA); het melden van content aan internetserviceproviders, met het vrijwillige verzoek tot verwijdering, onder verwijzing naar de eigen gebruikersvoorwaarden.
Binnen de politie is de opdracht voor de coördinatie en uitvoering belegd bij de Landelijke Eenheid, afdeling DLIO/ALI.

Het DO is al eerder geïnformeerd over het projectplan en de planning van de uitvoering. In het DO overleg van 28 maart 2016 is overeengekomen dat het project na afsluiting van elke fase in het DO wordt besproken. Met deze memo wordt het DO geïnformeerd over het verloop van de 1e fase van het project NL IRU en het vervolg. De belangrijkste punten zijn:

- In de 1e fase is het NTA-toetskader uitgewerkt, zijn afspraken gemaakt over het gezag en is het proces uitgewerkt en getest in de praktijk;
- Het belangrijkste knelpunt was het gebrek aan mensen en voorzieningen. Hierdoor kan er niet gestart worden met de uitvoering van fase 2 (1 september 2016 - 31 december 2016), waarin de ontwikkelde systematiek dient te worden gehanteerd en het NTA-proces dient te worden doorontwikkeld);
- Voor de schaarste in voorzieningen worden politie intern voor de korte termijn maatregelen getroffen om deze op te lossen. Voor het gebrek aan personeel zijn extra financiële middelen noodzakelijk om het project te kunnen voortzetten.

Resultaten

Testresultaten NTA proces

In de 1e operationele fase is het NTA-proces opgebouwd rondom [redacted]

10.2.G. + 10.2.C.

Gezag en toetsingskader

Er is afgesproken dat de NTA-meldingen wordt opgevat als strafrechtelijke handhaving van de rechtsorde onder gezag van het OM. Daarbij gaat het niet primair om *opsporing* en *vervolging*, maar om *voorkoming* en *beëindiging* van strafbare feiten.[2]

---

[1] 29 augustus 2014
[2] DO overleg van 28-03-2016 (NCTV, OM, AIVD, Politie)



In samenspraak met het OM is een toetskader opgesteld dat voorschrijft in welke gevallen NTA wordt toegepast. Conform dit toetskader wordt NTA beperkt tot (uitings)delicten waarop minstens 4 jaar gevangenisstraf is gesteld (art. 67 Sv-feiten). In de praktijk bleek dat dit kader fungeerde als een filter voor de bescherming van de vrijheid van meningsuiting. Zo is de NL IRU in de 1e projectfase door een groot aantal interne en externe partijen benaderd met verwijderingsverzoeken. Op grond van het toetskader is het merendeel van deze verzoeken *afgewezen*. In de 1e fase is de enorme behoefte aan kennis en kunde met betrekking tot blokkering en verwijdering van content gebleken.

Knelpunten

Personele Capaciteit

Bij de implementatie van maatregel 29 was de financiering van het project nog niet rond. Dit heeft consequenties gehad voor de uitvoering. In de eerste fase was er een kritiek gebrek aan personeel. Kernfuncties konden bovendien niet op het vereiste kwaliteitsniveau worden ingevuld. Voor de voortzetting van het project zijn extra fte noodzakelijk. Zonder voldoende gekwalificeerd personeel kunnen de gestelde doelen niet worden behaald (NTA-taak, expertise-opbouw & Identificatie van producenten en distributeurs).

Voor de uitvoering van de tweede en derde fase zijn conform projectplan in totaal 9 fte vereist.
De financiële middelen om extern personeel aan te trekken kunnen niet uit reguliere politiebudgetten worden gedekt. Het project NL IRU is niet in de inrichting van de Nationale Politie opgenomen en is gestart zonder toewijzing van financiële middelen. De oprichting van de NL IRU is in het project begroot op ca. € 0,9 mln., waarvan € 0,5 mln. personeelskosten. Als de unit structureel wordt, dan moeten de kosten in de reguliere budgettering worden meegenomen. Zonder personele invulling kan dit project niet worden voortgezet. Politie en DG Politie gaan in overleg over een oplossing voor dit punt.

Daarnaast is de benodigde expertise schaars. Een oplossing om op korte termijn voldoende gekwalificeerd personeel te vinden, wordt de ketenpartners in het DO gevraagd of zij op korte termijn medewerkers beschikbaar kunnen stellen met een WO of HBO werk- en denkniveau en (bij voorkeur) en ervaring met open source onderzoek die een periode van een half jaar (minimaal) bij de politie willen werken en bereid zijn tot grondige verdieping in de specifieke materie (zoals jihadisme, of rechts- of linksextremisme). Daarnaast is het van belang dat zij de Engelse taal voldoende beheersen en bij voorkeur nog een vreemde taal (Arabisch is zeer gewenst). Naast dat de IRU hierdoor op korte termijn operationeel kan worden, draagt deze integrale samenwerking bij aan het vergroten van kennis en kunde betreft de problematiek.

ICT-voorzieningen

In de eerste projectfase was er een kritisch tekort aan basisfaciliteiten, zoals bijvoorbeeld werkplekken. Voor aanvang van de tweede fase wordt dit politie intern middels herprioritering van middelen opgelost.

De automatisering had conform projectplan in een vergevorderd stadium moeten zijn. Om deze achterstand in te lopen is [redacted]
10.2.G Afspraken en financiering van softwareontwikkeling vanaf 2017 is nog onderwerp van gesprek. Dit heeft potentieel grote gevolgen voor automatisering van de NTA-taak.

Toezicht

In het bewindsliedenoverleg van 12-02-2016 heeft de minister van Veiligheid en Justitie aangegeven dat bij gebrek aan rechterlijke toetsing, er een vorm van onafhankelijk toezicht geregeld dient te worden met betrekking tot de uitvoering van de NTA-taak. Deze taak moet daarom buiten de uitvoerende partij belegd worden.

POLITIE

Bijlage: kosten specificaties

De oprichting van de NL IRU is in het project begroot op ca. € 0,9 mln., waarvan € 0,5 mln. personeelskosten. Als de unit structureel wordt, dan moeten de kosten in de reguliere budgettering worden meegenomen.

	Personeel	Functie LFNP	Aantal fte	Prijs	Totaal
	Internetmonitorspecialist	Senior Intelligence	3	3.518,43	€ 145.663,00
	Rechercheckundige	Operationeel expert Intelligence	2	3.518,43	€ 97.108,67
	Analist	Operationeel specialist B	1,5	4.191,21	€ 86.758,05
	Projectleider	Operationeel specialist C	1	4.737,84	€ 65.382,19
	Communicatiemedewerker	Bedrijfsvoeringsspecialist B	0,2	4080,83	€ 11.263,09
	Arabist	Operationeel specialist C	1	4.737,84	€ 65.382,19
	Jurist	Operationeel specialist C	0,5	4.737,84	€ 32.691,10
		Totaal fte	9,2		
	Hardware	**Werkplek**	**Aantal**		
		Kantoorautomatisering	[redacted]		
		[redacted]			
		dubbele 24 # monitoren (x2)			
10.2.g		[redacted]			
		Koptelefoon			
		[redacted]			
		Smartphone			
		Server			
		Microsoft Office			
		VPN router (10 poorten)			
		Glasvezelverbinding (1 GB)			
		TV on the wall (stelpost)			
	Tooling	Licentie Open mind			
10.2.g		Overige tooling (stelpost)			
	Opleidingskosten	[redacted]			
					PM
10.2.g	**Beheer**	Representatie		[redacted]	
		Gedrukte vakliteratuur e.d. (stelpost)			
		Abonnementen (stelpost)			
		Overige projectkosten			
	Reis- en verblijfskosten	Binnenland			
10.2.g		Bezoeken buitenlandse counterparts			
				Totaal generaal	€ 878.535,77

10.2e
Van: [redacted]
Aan:
Cc:
Onderwerp: FW: aanvulling IRU
Datum: dinsdag 18 december 2018 21:23:39

10.2e
Ha [redacted]
In het stukje dat ik je aangeleverd heb voor de verantwoording stond nog een PM inzake de IRU.
Kreeg zojuist daar input op. Heb nog weer nagevraagd of dit gedubbel checkt is met DGPOL maar nog geen reactie.
Weet ook niet of onderstaande info helemaal bruikbaar is maar dan weet je iig wat er ligt aan potentiele info en dat hier nog aan gewerkt wordt.

10.2e [redacted]
Groet [redacted]

10.2e
Van: [redacted]
Verzonden: dinsdag 18 december 2018 14:46
Aan: [redacted]
Onderwerp: aanvulling IRU

Hoi [redacted]
Afgelopen jaar is er een start gemaakt met de IRU.
In de eerste helft van het jaar is de energie uitgegaan naar het procesontwerp, de implementatie daarvan, en het werven van medewerkers.
[redacted]
Met deze groep is een begin gemaakt om het proces van de internet referral unit op te starten.

NTA-proces
Het NTA-proces is uitgedacht, afgestemd met samenwerkingspartners en in werking getreden en gaande weg aangepast en aangescherpt. Het resultaat daarvan is dat er 1234 URL's in 2018 zijn opgespoord.
Daarnaast hebben we als IRU ook deelgenomen aan een aantal actiedagen van Europol waarbij we
10.2c/10.2g ook [redacted] hebben gereferd. Aantallen daarvan hebben we niet inzichtelijk omdat het rechtstreeks via Europol is gegaan.
10.2c/10.2g
10.2g
[redacted]

Samenwerking met Europol algemeen
10.2.g Ook met Europol is in algemene zin samengewerkt; [redacted]
10.2.g

Met vriendelijke groet,

10.2e [redacted]

Politie | Landelijke Eenheid | DLIO | Afdeling Landelijke Informatie

Hoofdstraat 54, 3972 LB Driebergen
Postbus 100, 3970 AC
10.2e [redacted]


10.2e [redacted]

10.2e **Van:** [redacted]
Verzonden: maandag 28 september 2020 10:49
10.2e **Aan:** [redacted]
Onderwerp: RE: IRU plannen, geld en toekomst
Bijlagen: stand van zaken IRU 2019.pdf

Dit is wat ik weet over de osinteenheid:
"De IRU is met RA geld volgens de opdrachtbrief van maart 2019 ingericht en structureel opgenomen in de
formatie van ALl/Team OSint (Open bronnen) bij DLIO. [redacted]

10.2g/ 10.2c

[redacted] Verder heb ik geen info over wat voor werkzaamheden zij uitvoeren.

Van: [redacted]
Verzonden: maandag 28 september 2020 10:43
10.2e **Aan:** [redacted]
CC: [redacted]
Onderwerp: RE: IRU plannen, geld en toekomst

Nabrander:

10.2g/ 11.1 [redacted]

Groeten,

10.2e [redacted]

Van: Schilt, drs. S. van - BD/PNI
Verzonden: maandag 28 september 2020 10:37
Aan: Ariës, R.E.M. - BD/PACT <r.e.m.aries@nctv.minjenv.nl>
CC: Mos, S.C.J. - BD/PNI <s.c.j.mos@nctv.minjenv.nl>
Onderwerp: RE: IRU plannen, geld en toekomst

10.2e [redacted]

11.1 [redacted]

10.2e Even teruggrijpend op ons telefoongesprek, heb ik ten behoeve van het gesprek met [redacted] nog een aantal aandachtspunten:

- De oorspronkelijke IRU (2016) was een pilot. De taak en rol van de IRU was – in ieder geval op hoofdlijnen – tamelijk onomstreden. Zie ook bijgaand persbericht van de politie.

https://www.politie.nl/nieuws/2017/januari/13/nieuwe-politie-unit-bestrijdt-jihadistische-content.html

- In het bestedingsplan van 13 mln CT geld is ten aanzien van de IRU en de internetaanpak het volgende opgenomen: [redacted]

10.2g/ 10.2c

- Van de taken die IRU nu doet, zijn er twee direct gerelateerd aan het IRU werk (NTA en Europol, tenminste als het gaat om de samenwerking met de Europol Internet Referral Unit) en 1 met de afspraken die zijn gemaakt (deelname aan het programma, [redacted].

11.1

- De andere twee: analyse, early warning en bijlopen operationeel CTER zijn niet gerelateerde taken.

10.2g

10,2g/ 11.1

- [redacted]

10.2g/ 11.1 [redacted]

10.2g/ 11.1 [redacted]

10.2g/ 11.1 [redacted]

10.2e Denk dat dit ook nuttige info is voor [redacted], maar wilde eerst even jullie reactie peilen.

Met vriendelijke groet,

10.2e [redacted]

10.2e **Van:** [redacted]
Verzonden: donderdag 24 september 2020 17:38
Aan: [redacted]
10.2e **CC:** [redacted]
Onderwerp: IRU plannen, geld en toekomst

10.2e Dag [redacted],
[redacted] en ik zijn bezig met een financiële verkenning voor implementatie van de TCO verordening. We delen graag –op een ander moment- de inzichten die dat oplevert.
In dat kader spreken we ook het IRU potje aan en voeren we al een langere periode het gesprek hierover met de politie (LE, portefeuille en DGP&V).

Vanwege het door de autoriteit overnemen van de referral taak was onze verwachting was dat er per 2022 een flink bedrag structureel over zou komen naar de autoriteit. Wij dachten aan ongeveer 1 miljoen per jaar.
Nu lijkt dit te gaan om 4 a 5 ton. De reden hiervoor is dat wij aannamen dat de referral taak een groot deel van de IRU behelsde, maar dit lijkt niet zo te zijn. En dat komt omdat de IRU (zo lijkt het althans) gedurende de afgelopen jaren haar IRU taak anders dan initieel bedoelt is gaan invullen en uitvoeren. Die vrijheid is er geweest, en er is bij oprichting van de IRU ook geen opdrachtbrief verstuurd aan de politie.

Wij willen graag met jou een 2-tal vragen bespreken.

11.1 • [redacted]

10.2e [redacted] en ik zouden hier graag kort met je over willen praten. 1 oktober gaan wij weer verder in gesprek met DGP&V en de LE.
Hopelijk kunnen we voor die tijd een richting bepalen met elkaar. Anders later! Wil je dat ik een moment in onze agenda's plan?

In de bijlage een schets van de initiële opdracht en de huidige opvattingen van de politie inz IRU taak (met dank
10.2e aan [redacted]).

10.2e Mvgr [redacted]

Tussentijdse stand van zaken IRU politie eind oktober 2019

10.2g/ 10.2c

De IRU richt zich op detectie en duiding van online jihadistische content, [redacted](Notice & Take Action). De oprichting komt voort uit een politiek geprioriteerde opdracht, maatregel 29 uit het Actieprogramma Integrale Aanpak Jihadisme (aug. 2014) en valt onder de verantwoordelijkheid van de Portefeuillehouder CTER. De IRU werkt samen met zusterdiensten aan een gemeenschappelijke Europese taak. In deze Europese samenwerking moet de IRU haar aandeel kunnen (blijven) dragen. Sinds september 2017 is de IRU operationeel met [redacted]. Van de aan de IRU toegekende versterkingsgelden (€1.7 mln) wordt een uitbreiding gerealiseerd naar [redacted]. Deze uitbreiding heeft op 14 augustus 2018 de besluitvorming van het ELO-F gepasseerd. [redacted].

10.2g/ 10.2c

10.2g/ 10.2c

Vanaf 2019 is toegewerkt naar een platform voor een multidisciplinaire internetaanpak om de digitale weerbaarheid en aanpak extremisme online te versterken. Hiervoor is een beperkt deel van de versterkingsgelden begroot: [redacted].

10.2g/ 10.2c

In de definitieve brief van DGPenV ontvangt de politie een betaling van €1.7 mln. per jaar vanaf 2018 [redacted].

10.2g/ 10.2c

[redacted].

10.2g/ 10.2c

Toekomstvisie IRU

In september 2019 is met de Eenheidsleiding van de LE, hoofd DLIO, de TC ALI en de CTER portefeuille stilgestaan bij de stand van zaken binnen de IRU en is de behoefte uitgesproken aan een heldere toekomstvisie mbt de IRU werkzaamheden. Op hoofdlijnen houden de IRU medewerkers zich nu met de volgende zaken bezig:

- NTA proces
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- Deelname en bijdrage aan et Programma Online Samenwerking van de NCTV (samen met KMar, AIVD en MIVD)

10.2g/ 10.2c

De referal (NTA) taak [redacted]. Ten aanzien van die taak zien we de afgelopen tijd een enorme afname van zichtbare content. [redacted] Met een aanstaande, verplichte verwijdering van content (NTD) in het kader van de EU verordening is het voorts onduidelijk of er überhaupt nog behoefte aan en ruimte is voor vrijwillige verwijdering. [redacted].

10.2g/ 10.2c

10.2g/ 10.2c

Vraag en antwoord

	Onderwerp	Nederlandse internet referral unit
	Dossierhouder	[redacted]
10.2e	Bereikbaarheid	[redacted]
	Minister	VenJ

Vraag

Wat is de stand van zaken van de Nederlandse internet referral unit?

Antwoord

- De eerste operationele fase (1 maart 2016 - 31 augustus 2016) van de Internet Referral Unit (NL IRU) is geëvalueerd.

10.2.g. & 10.2c
- [redacted] Het project is na afronding van de 1e fase door de stuurgroep teruggezet naar de initiatiefase.
- De IRU krijgt een financiële impuls en doorstart. VenJ voert hierover overleg met de Nationale Politie.
- Het werkproces voor Notice and Take Action (NTA; het melden van content aan internetserviceproviders, met het vrijwillige verzoek tot verwijdering, onder verwijzing naar de eigen gebruikersvoorwaarden) is ontwikkeld en casuïstiek is behandeld.
- In samenspraak met het OM is vastgesteld in welke gevallen NTA wordt toegepast. Deze afbakening van gevallen dient ter bescherming van de vrijheid van meningsuiting. Zo wordt NTA beperkt tot (uitings-)delicten waarop minstens 4 jaar gevangenisstraf is gesteld.



Ministerie van Veiligheid en Justitie

AO 17 november 2016
JBZ-Raad 18 november 2016

Contactpersoon

Naam [redacted]
tel.nr. [redacted]

Vraag

Wat is de stand van zaken van de Nederlandse internet referral
10.2e unit?

Antwoord

- De eerste operationele fase (1 maart 2016 - 31 augustus 2016) van de Internet Referral Unit (NL IRU) is geëvalueerd.
- 10.2g [redacted]
- De IRU krijgt een financiële impuls en doorstart. VenJ voert hierover overleg met de Nationale Politie.
- Het werkproces voor Notice and Take Action is ontwikkeld en casuïstiek is behandeld.
- Notice and Take Action is het melden van content aan internetserviceproviders, met het vrijwillige verzoek tot verwijdering, onder verwijzing naar de eigen gebruikersvoorwaarden
- In samenspraak met het OM is vastgesteld in welke gevallen Notice and Take Action wordt toegepast. Deze afbakening van gevallen dient ter bescherming van de vrijheid van meningsuiting.
- Zo wordt Notice and Take Action beperkt tot (uitings-)delicten waarop minstens 4 jaar gevangenisstraf is gesteld.

Vraag: Wat doet het kabinet op dit moment aan activiteiten omtrent de aanpak van illegale content?

- Voor NL is het van essentieel belang dat de verwijdering van terroristische content mogelijk is van alle online fora, groot en klein, nu en in de toekomst.

- De inrichting van een *Internet Referral Unit (IRU)* was een eerste stap in de actieve detectie van terroristische content.

- Om deze aanpak verder uit te bouwen en de samenwerking tussen de betrokken overheidspartijen te bevorderen heeft dit kabinet besloten om per 2018 structureel 3 miljoen euro te investeren in de integrale multidisciplinaire aanpak van extremistisch en terroristisch gebruik van digitale media.

- Onderdeel van deze aanpak is ook het verkennen en nader bezien van nieuwe innovatieve manieren van online interventies.

- Ook faciliteert en steunt de Nederlandse overheid alternatieve boodschappen door personen en/of organisaties die geloofwaardig zijn voor de doelgroep.

- De concept verordening kan een prima aanvulling zijn op deze nu lopende aanpak.

Vraag: Hoe staat het met de Internet referral unit van Europol?

- Vanaf 1 juli is bij Europol een Internet Referral Unit operationeel.
- Deze unit is mede op mijn verzoek gecreëerd met een resolutie van de JBZ-raad na de aanslagen in Parijs.
- De Europol Referral Unit richt zich op de aanpak van terroristisch materiaal op het internet, bijvoorbeeld op officiële IS- en al Qai'da-uitingen uit Syrië en Irak.
- In de periode januari t/m maart 2018 zijn door de Internet Referral Unit van Europol **5708 verwijderingsverzoeken uitgestuurd**. 61% bleek ook daadwerkelijk te zijn verwijderd.

Vraag: Hoe staat het met de Internet referral unit in NL?

- De overheid werkt op nationaal en internationaal niveau aan het tegengaan van de verspreiding van extremistische uitingen.

- Onderdeel hiervan is de Internet Referral Unit van de politie die jihadistische en/of extremistische content laat verwijderen door internetbedrijven.

- In de periode januari t/m maart 2018 zijn door de Nederlandse Internet Referral Unit **330 verwijderingsverzoeken uitgestuurd**. 69% bleek ook daadwerkelijk te zijn verwijderd.

10.4. Online aanpak / opruiing

Factsheet aanpak online

- De strafrechtelijke aanpak van (extremistische) uitingen is gericht op vervolging en bestraffing van een (natuurlijk) persoon en heeft niet (zoals de TCO verordening) tot doel het tegengaan van verspreiding van terroristische inhoud.
- Wanneer het gaat om uitingen die **aanzetten tot haat**, **opruien tot het plegen van strafbare feiten**, **werven voor de gewapende strijd** of waarmee personen worden **bedreigd of beledigd** is het mogelijk om strafrechtelijk te vervolgen.
- Hierbij is sprake van spanning tussen de strafbaarstelling van extremistische boodschappen enerzijds en de vrijheid van meningsuiting anderzijds.
- Het recht op vrijheid van meningsuiting houdt op daar waar uitingen de inhoud aannemen van belediging, werven voor de gewapende strijd, aanzetten tot haat, opruiing of bedreiging.

Vervolging van (extremistische) uitingen

- In het kader van de beoordeling van extremistische uitingen zijn de belangrijkste strafbepalingen die inzake groepsbelediging (artikel 137c Sr), aanzetten tot haat, discriminatie of geweld (artikel 137d Sr), opruiing (artikelen 131 en 132 Sr), werven voor de gewapende strijd (artikel

205 Sr), eenvoudige belediging (artikel 266 Sr) en bedreiging (artikel 285 Sr).

- Bij beoordeling van de strafbaarheid van uitingen, wordt onderzocht of een uiting valt onder de delictsomschrijvingen van de genoemde misdrijven.
- Bij de beoordeling van uitingsdelicten speelt de context een belangrijke rol. Zo heeft de Hoge Raad bepaald dat de strafbaarheid van uitingen afhankelijk is van de aard van de uitlatingen, de eventuele onderlinge samenhang tussen verschillende uitingen en de context waarin de uitlatingen zijn gedaan (Hoge Raad 22 december 2009, NJ 2010/671).
- De context van de uiting is nog in een ander opzicht van (groot) belang bij de beoordeling van de strafbaarheid van uitingsdelicten. Bij de bepaling van de strafbaarheid van (groeps-)belediging en het aanzetten tot haat dient te worden bekeken of met uitingen die in beginsel onder de delictsomschrijving vallen, een deelname aan het publieke debat is beoogd die in verband met het recht op vrijheid van meningsuiting bescherming verdient.

Verwijderen online content

- De aanpak die de *Internet Referral Unit* (NL IRU) hanteert, is gebaseerd op de methode *Notice and Take Action* (NTA): het identificeren, duiden en melden van bepaalde content aan internetbedrijven, met het oog op verwijdering. De werkwijze van de IRU is beperkt tot strafbare feiten waarop tenminste 4 jaar gevangenisstraf is gesteld (art. 67 Sv

feiten). Hieronder vallen de **uitingsdelicten opruiing en werven voor de gewapende strijd**. Voor de vraag wanneer (jihadistische) content past binnen de voorwaarden die gelden voor deze delicten is vooral gekeken naar jurisprudentie ontleend aan de Context zaak.

- Wanneer de NL IRU melding maakt van de aanwezigheid van content die aan de criteria voldoet, verzoekt de NL IRU de provider de betreffende content te beoordelen in het licht van de eigen gebruikersvoorwaarden.
- In die gevallen waarin de NTA-gedragscode niet afdoende is voor de verwijdering van de gegevens, bijvoorbeeld omdat verschil van inzicht bestaat over de strafbaarheid daarvan, of wanneer sprake is van een aanbieder die de gedragscode niet heeft ondertekend, kan de officier van justitie gebruikmaken van de bevoegdheid in art. 125p Sv.
- Art. 125p Wetboek van Strafrecht voorziet in de bevoegdheid een aanbieder van een communicatiedienst te bevelen gegevens, aangetroffen tijdens het onderzoek in een geautomatiseerd werk, met betrekking tot welke of met behulp waarvan het strafbare feit is gepleegd, ontoegankelijk te maken.
- Hiermee wordt bereikt dat een strafbaar feit wordt beëindigd of een nieuw strafbaar feit voorkomen. Het bevel tot ontoegankelijkmaking van gegevens is beperkt tot gevallen waarin sprake is van verdenking van een misdrijf waarvoor voorlopige hechtenis mogelijk is.

- Deze bevoegdheid kan dus slechts gebruikt worden op gegevens die bij een doorzoeking in een geautomatiseerd werk worden aangetroffen. Bovendien moet tussen de gegevens en een strafbaar feit een bepaald verband bestaan, te weten: het moeten gegevens zijn met betrekking tot welke of met behulp waarvan het strafbare feit is gepleegd.

Q: Bij de aanslag op Paty lijkt berichtgeving op internet de dader te hebben gemotiveerd. Is er een direct verband tussen deze berichtgeving en de aanslag?

A:

- In de berichtgeving over de aanslag op Paty wordt de rol van sociale media benadrukt.
- Of een causaal verband bestaat tussen de discussie op sociale media en de aanslag, is niet aan mij om te beoordelen.
- Het is aan de Franse justitie om te onderzoeken of de vader, het moskeebestuur en andere verspreiders van deze berichten strafrechtelijk aansprakelijk kunnen worden gesteld.

Achtergrond

- De vader van een van de leerlingen filmpjes heeft op facebook geplaatst waarbij Paty met naam en toenaam genoemd, waarin gevraagd werd om diens ontslag en waarin werd gedreigd met demonstaties voor de school en klachten bij de inspectie.
- Ook heeft de voorzitter van het moskee bestuur een video tegen Paty op de website van een moskee gedeeld.

Q: Kunnen personen die extremistische uitingen op internet plaatsen in Nederland worden vervolgd?

A

- Ja. In Nederland kunnen personen die extremistische uitingen op internet plaatsen strafrechtelijk vervolgd worden door het Openbaar Ministerie.
- Het betreft hier onder meer:
  - uitingen waarmee personen bedreigd en/of beledigd worden,
  - uitingen die aanzetten tot haat, discriminatie of geweld
  - uitingen die opruien tot het plegen van strafbare feiten
  - en uitingen die werven voor de gewapende strijd.
- Bij het beoordelen van de strafbaarheid wordt natuurlijk gekeken naar het spanningsveld tussen de inhoud van extremistische boodschappen enerzijds en de vrijheid van meningsuiting anderzijds.

Q: Kunnen uitingen op sociale media, zoals de content tegen Paty, in Nederland van het internet worden verwijderd?

A

- Ja. De *Internet Referral Unit* van de Nationale politie, de IRU, kan extremistische content identificeren en internetbedrijven via Europol verzoeken deze te verwijderen. Dit is de *Notice and Take Action* procedure.
- Dit is gericht op het schonen van het internet door het verwijderen van extremistische uitingen en specifiek op opruiing en werven voor de gewapende strijd.
- Daarnaast kan de officier van justitie in geval van verdenking van een misdrijf aan een communicatiedienst bevelen om bepaalde gegevens ontoegankelijk te maken.
- Hierbij kan worden gedacht aan teksten die opruiend zijn en/of teksten die gelegenheid, middelen of inlichtingen verschaffen tot het plegen van een terroristische misdrijf.
- Ook content die als discriminatie kan worden geoormerkt kan worden verwijderd. Voor discriminatie is er het Meldpunt internetdiscriminatie, dat als 'trusted flagger' strafbare content kan melden bij de grote internetplatformen en providers kan aanspreken.

Q: hoe wordt de verordening Terroristische Content Online- in NL geïmplementeerd (ZBO)?

A:

- De verordening vereist dat iedere lidstaat een competente autoriteit opricht of aanwijst.
- De competente autoriteit is bevoegd om verwijderbevelen uit te vaardigen, om specifieke maatregelen af te dwingen en om sancties uit te vaardigen tegen hostingproviders.
- De wijze waarop Nederland invulling gaat geven aan de verordening hangt af van hoe de definitieve verordening eruit komt te zien.
- Maar gelet op de fase van de onderhandelingen in Brussel en de korte implementatie termijn van 12 maanden tref ik alvast de nodige voorbereidingen.
- Zo heb ik met de staatssecretaris van Binnenlandse Zaken overlegd over de juridische grondslag en de inrichting van de toekomstige autoriteit.
- Beiden zijn wij van mening dat de status van Zelfstandig Bestuursorgaan voor deze nieuwe autoriteit opportuun is.
- Dit zal ik nader onderbouwen in de Nederlandse uitvoeringswetgeving. Ik zal het wetgevingsproces starten zodra de finale tekst van de verordening is gepubliceerd.

IRU-gelden 2014 - heden

Kern:

11.1/10.2g
- De IRU (aanvankelijk 13 FTE) zijn bij RA gelden structureel gefinancierd. [redacted]
- Door de komst van de Autoriteit, die verwijderverzoeken kan uitvaardigen, lijkt het logisch en is dit inmiddels ook al enige tijd een gedeelde mening, dat dus de 'verwijderverzoeken/referral taak' van de IRU over gaat naar de Autoriteit. [redacted]
11.1
 In het kader van hoeveel geld kan de IRU straks structureel (per 2022) overhevelen naar de Autoriteit worden al geruime tijd gesprekken gevoerd met de LE (portefeuille) en DGP&V en volgen zij de redernering: financiën volgen de taak.

11.1/10.2g
- [redacted]

Achtergrond & analyse:

Oprichting IRU 2014: het oorspronkelijke idee

De IRU richt zich op detectie en duiding van online jihadistische content, identificatie van producenten en verspreiders en melding van strafbare content (Notice & Take Action). De oprichting komt voort uit een politiek geprioriteerde opdracht, maatregel 29 uit het Actieprogramma Integrale Aanpak Jihadisme (aug. 2014) en valt onder de verantwoordelijkheid van de Portefeuillehouder CTER.

Maatregel 29. Bestrijden van verspreiding van radicaliserende, haatzaaiende jihadistische content.

a) Betrokken burgers kunnen jihadistische (terroristische, haatzaaiende en geweldverheerlijkende) content op internet en sociale media melden.
b) Producenten en verspreiders van online jihadistische propaganda en de digitale platforms die zij misbruiken worden geïdentificeerd.
c) Deze informatie wordt actief gedeeld met de handelingsbevoegde instanties en relevante dienstverleners (waaronder internetdiensten).
d) Een specialistisch team van de Nationale Politie bestrijdt online jihadistische content. Dit team licht het OM in over mogelijke strafbare uitingen (onder bestaande uitingsdelicten). Als toepassing van de vrijwillige gedragscode niet leidt tot verwijdering, kan een strafrechtelijk bevel volgen. In het wetsvoorstel computercriminaliteit III wordt voorgesteld deze procedure verder te verbeteren (Notice and Take Down).
e) Dit team maakt afspraken met internetbedrijven over effectieve blokkeringen en verzorgt verwijzingen ter beoordeling van de content tegen de eigen gebruikersvoorwaarden (Notice and Take Action).
f) Internetbedrijven die volharden (na attendering) in het faciliteren van 'geliste' terroristische organisaties door het verspreiden van jihadistische content, worden aangepakt hetzij op basis van een aanpassing van EU-verordening 2580/2001 in samenhang met de nationale sanctieregeling terrorisme 2002, hetzij op basis van nader tot stand te brengen nationale regelgeving.
g) Het specialistisch team monitort zelfstandig, maar werkt nauw samen met het online burgermeldpunt.

h) Er wordt een geactualiseerde lijst van online jihadistische (sociale media) websites gepubliceerd. Deze lijst kan onder andere door gemeenschappen, professionals en ouders gebruikt worden hun omgeving te waarschuwen.

Wat de IRU nu doet:
In september 2019 heeft de politie stilgestaan bij de toekomstvisie van de IRU, en zijn de volgende werkzaamheden gedefinieerd:

- NTA proces

10.2c/ 10.2g

[redacted]

- Deelname en bijdrage aan et Programma Online Samenwerking van de NCTV (samen met KMar, AIVD en MIVD)

Voortgangsrapportages
In 2014 zijn de IRU-gelden aan de politie toegewezen in verband met maatregel 29 uit het actieprogramma. Uit de voortgangsrapportages die we ter beschikking hebben, lopend van december 2014 tot en met september 2016 wordt duidelijk dat de volgende zaken in afstemming met de NCTV zijn gebeurd.

- NTA proces inregelen en doorontwikkelen
- Tweesporenbeleid jihadistische content: producenten/verspreiders identificeren/aanpakken & samenwerken met sociale-mediabedrijven/internet service providers
  - Nb onduidelijk wat early warning op thema Jihadisme (en CTER) in houdt, maar wellicht valt dat hieronder.
- Politie levert een specialist aan Europol tbv het daar lopende internet traject
- Bijlopen operationele CTER onderzoeken

11.1/ 10.2g

[redacted]

Van: [redacted]
Aan:
10.2e **Onderwerp:** FW: Uitkomst IRU-gelden en -taken politie
Datum: woensdag 14 oktober 2020 14:07:23

Van: [redacted]
Verzonden: dinsdag 6 oktober 2020 12:55
10.2e **Aan:** [redacted]
CC: [redacted]
Onderwerp: RE: Uitkomst IRU-gelden en -taken politie

10.2e Hoi [redacted],

10.2.G & 10.2.C Gelet op het structurele karakter van de gelden voor de IRU hebben we afgelopen overleg vooral met elkaar doorgesproken over de vraag [redacted]

Kijkend naar de huidige tekst van de Verordening ligt het in de lijn der verwachting dat de referraltaak overgaat naar de bevoegde autoriteit. Dit is wat ons betreft een goede ontwikkeling nu dit geen specifieke politietaak is: iedere burger kan in principe een dergelijk verzoek doen. Met het overgaan van de referraltaak blijft de politie met de resterende taken een belangrijke bijdrage leveren aan de CTER aanpak vanuit de politietaak.

Hoewel de naamgeving anders doet vermoeden is in de afgelopen jaren de referraltaak binnen/van de IRU een steeds kleiner onderdeel geworden van de werkzaamheden. Anderzijds vragen nieuwe (online) ontwikkelingen juist meer aandacht en inzet van de politie (in samenwerking met OSInt) waarbij de kennis en expertise binnen de IRU onmisbaar is. Bijvoorbeeld waar het gaat om de verbreding van focus van jihadistische content naar extremistische content (links, rechts, klimaat, etc.). De werkzaamheden binnen de IRU zijn in de loop der tijd ook meegegroeid met de veranderende vraag vanuit de CTER aanpak. Om deze taak te kunnen blijven uitvoeren vanuit de politie is behoud van de huidige CTER kennis en expertise - en structurele financiering daarvan - nodig.

Naast de borging van de benodigde online kennis en kunde/ de intelligence functie binnen de politie is [redacted] Daarbij dient te worden gekeken hoe de politie (met andere partners) straks samenwerkt met de autoriteit. In de verkenning die de NCTV eerder heeft opgesteld met de betrokken partners wordt gesteld dat onderzocht moet worden hoe de huidige taken, expertise en netwerken van de IRU van pas kunnen komen bij de opzet, implementatie en operationalisering van de autoriteit. Bezien dient te worden hoe de OSInt-werkzaamheden van de politie (primair gericht op opsporing en verzameling van intelligence) de werkzaamheden van de autoriteit kunnen versterken in de bestuursrechtelijke aanpak en vice versa. Het samenwerkingsprogramma Online kan hierbij een belangrijke rol vervullen.

10.2.G. en 10.2.C

Concreter kun je qua activiteiten binnen de IRU, naast de referrals, onder meer denken aan:

10.2.G. & 10.2.C

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
    - [redacted]

Mvg,

10.2e [redacted]

Van: [redacted]
Verzonden: vrijdag 2 oktober 2020 13:41

10.2e **Aan:** [redacted]
CC: [redacted]
Onderwerp: RE: Uitkomst IRU-gelden en -taken politie
Hoi [redacted],
Wij gaan zoals besproken een opzet maken voor de nota om e.e.a. verder te bespreken. We hebben elkaar nu al best vaak gesproken over de huidige IRU taken, en de 'ophaalsessie' waar je afgelopen weken/maanden mee bezig bent geweest.
Zou je voor ons als bijlage bij de nota 1 a4 kunnen opmaken met een goede beschrijving van de huidige IRU taken? Of heb je dat wellicht al? Dan ontvangen we dat graag!

Fijn weekend alvast,
Gr [redacted]
-----Oorspronkelijke afspraak-----
10.2e **Van:** [redacted]
Verzonden: donderdag 10 september 2020 15:02
Aan: [redacted]
Onderwerp: Uitkomst IRU-gelden en -taken politie
Tijd: donderdag 1 oktober 2020 09:00-10:00 (UTC+01:00) Amsterdam, Berlijn, Bern, Rome, Stockholm, Wenen.
Locatie: Webex
Verschuiving naar de ochtend om agendapassend te maken!

Beste collega's,
Ik plan graag dit moment in om de uitkomst te bespreken over welke taken er nog achter blijven bij de politie met de oprichting van de CA en wat dat betekent voor de IRU-gelden.
10.2e Ik weet niet zeker of [redacted] de taken van [redacted] dan al helemaal heeft overgenomen, dus voor de zekerheid naar jullie beiden de uitnodiging verzonden. Als een iemand aanschuift is dat natuurlijk voldoende.
10.2e Met vriendelijke groet,
[redacted]



National Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Dep. VERTROUWELIJK
NCTV

Programma Versterken Contraterroisme keten - nationaal en internationaal

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
[redacted]

10.2e

Datum
30 april 2021

Ons kenmerk
x

nota

Gespreksnotitie over wijze van implementatie TOI-verordening

Aanleiding

De Raad van Ministers van de EU en het Europees Parlement hebben een akkoord bereikt over de verordening voor het tegengaan van de verspreiding van terroristische online-inhoud (TOI-verordening). Deze is op 17 mei jl. gepubliceerd en kent een implementatietermijn van een jaar (vanaf 7 juni). Voortvloeiend uit de verordening, dienen EU-lidstaten, waaronder NL, een autoriteit in te richten die gaat optreden tegen verspreiding van terroristische online-inhoud. In NL wordt deze taak gecombineerd met de aanpak van kinderpornografische online-inhoud.

Doel

De uitvoeringswet voor de implementatie van de TOI-verordening in NL is in voorbereiding en wordt in de eerste helft van juni naar de minister verstuurd voor akkoord, waarna de volgende stappen in het wetgevingsproces worden genomen. Met dat vooruitzicht stellen we u graag op de hoogte van de stand van zaken rond de implementatie en brengen we een aantal specifieke punten onder uw aandacht. Hiervoor is een kort overlegmoment gepland op donderdag 3 juni om 9.30 uur. Deze gespreksnotitie dient ter kennisname en toelichting voor deze bespreking.

Update

- Na de implementatietermijn van ca. 1 jaar dienen alle EU-lidstaten de autoriteit operationeel te hebben. Ook de Nederlandse uitvoeringswetgeving dient binnen een jaar gereed te zijn. Voor dit wetgevingstraject geldt dat er maar beperkte mogelijkheden zijn tot versnelling om de 12-maanden-termijn te halen, maar uiteraard worden de mogelijkheden die er zijn benut, zie bijlage 1 voor de planning.
- 10.2e Vanuit ABD-interim is [redacted] als kwartiermaker aangesteld. [redacted] gaat samen met het nog samen te stellen kwartiermakersteam (bestaande uit circa 10 FTE) en de beleidsteams vanuit NCTV en DRC zorgdragen voor de oprichting van de nieuwe autoriteit. De directeur CT en de directeur DRC (directie rechtshandhaving en criminaliteitsbestrijding) zijn opdrachtgevers van de kwartiermaker.
- De in te richten autoriteit zal in 2022 (opstartjaar) naar verwachting een
10.2g bezetting van [redacted] (TOI en kinderpornografisch materiaal); In de jaren daarna zal naar verwachting de autoriteit de gewenste mate van samenwerking met de nationale sectorpartijen, inlichtingen- en opsporingsinstanties en internationale partners onderhouden [redacted]
10.2g
- Eerder is overeengekomen dat de autoriteit in NL als ZBO wordt ingericht. Eenmaal operationeel wordt de autoriteit aangestuurd middels het besturingsmodel van J&V. Hierin is de SG de eigenaar, de NCTV en DGRR de opdrachtgevers en de autoriteit de opdrachtnemer. Jaarlijks

verstrekken de opdrachtgevers een beleidsmatige opdracht aan de nieuwe autoriteit. De opdrachtgevers zijn tevens budgethouder en sturen en houden toezicht op de uitvoering van afzonderlijke opdrachten die worden uitgevoerd door de autoriteit als opdrachtnemer. De NCTV dient hiervoor capaciteit in te richten vanaf 2022.

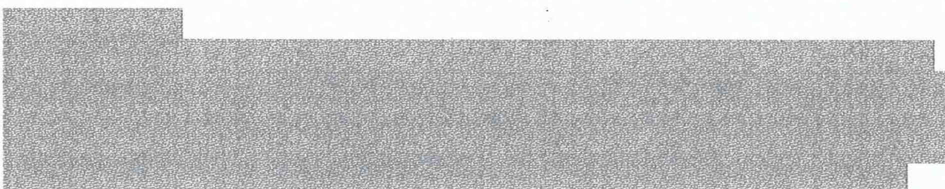
- Daarnaast geldt dat de autoriteit voor de wettelijke taken onafhankelijk zal opereren, conform de Kaderwet zelfstandig bestuursorganen en de in voorbereiding zijnde Uitvoeringswet verordening terroristische online-inhoud en nationale wetgeving voor het tegengaan van kinderporno-grafische online-inhoud.
- De afgelopen maanden is geïnventariseerd van welke financieringsbronnen gebruik gemaakt kan worden om de autoriteit (structureel) te bekostigen. De NCTV en DGRR voorzien gebruik te kunnen maken van de volgende 3 bronnen, waarmee de financiering tot 2027 dekkend is:
    - Internet Referral Unit (IRU) onderbesteding middelen aan NP sinds 2018 - terug naar NCTV
    - Claim NCVT
    - Claim DGRR
    - Internal Security Fund (ISF) Europese subsidie voor NCTV
    - Internal Security Fund (ISF) Europese subsidie voor DGRR|

Gesprekspunten

Bestuur autoriteit
De in te richten autoriteit zal een bestuur krijgen van 3 leden. Dit bestuur is primair verantwoordelijk voor de dagelijkse aansturing van de autoriteit. Voorgesteld wordt evenwel om de voorzitter van het bestuur een zwaarder profiel te geven en een functionaris aan te stellen die waar nodig, ook naar buiten toe, met gezag de autoriteit kan vertegenwoordigen en de keuzes van de autoriteit omtrent het wel of niet verwijderen van content kan toelichten. Dit vanwege de maatschappelijke en politieke aandacht voor het reguleren van onwenselijke uitingen op internet en het spanningsveld met de vrijheid van meningsuiting.

Rol en karakter autoriteit
De autoriteit heeft tot taak het ontoegankelijk maken van terroristische online-inhoud te bevorderen en op deze wijze de verspreiding van deze inhoud via internet tegen te gaan. Beoogd wordt een autoriteit die niet louter verbiedt en laat verwijderen, maar die ook een samenwerkingspartner is voor de internetsector en bemiddelaar tussen ogenschijnlijk tegengestelde belangen: een schoon internet en een open internet. Een schoon internet door het beschermen van burgers tegen illegale content, rekening houdend met opsporings- en inlichtingenbelangen. Een open internet door het waarborgen van fundamentele rechten, zoals de vrijheid van meningsuiting. De autoriteit hanteert een hybride aanpak: zij werkt via (horizontale) relaties samen met aanbieders van hostingdiensten. Waar dat (nog) niet voldoende effect sorteert, vervult zij een (verticale) toezichthoudersrol en zal zij zo nodig maatregelen nemen zoals het uitvaardigen van verwijderbevelen en als ultimum remedium sanctioneren.

10.2g


[redacted]

[redacted]

Verwijderingsbevelen en laten vervallen van verwijderingsverzoeken
De TOI-verordening bepaalt dat een autoriteit in een EU-lidstaat een verwijderingsbevel kan sturen naar een aanbieder van een hostingbedrijf gevestigd in de EU. Dit is een nieuw instrument dat aanbieders van hostingdiensten verplicht om terroristische inhoud zo spoedig mogelijk te verwijderen of te blokkeren en in elk geval binnen één uur na ontvangst van het verwijderingsbevel.

De TOI-verordening laat ruimte om als EU-lidstaat naast verwijderingsbevelen ook verwijderingsverzoeken te sturen, maar regelt er niets over. Het instrument van verwijderingsverzoeken is dan ook niet nodig om aan de verordening uitvoering te geven. Een verwijderingsbevelen heeft een verplicht karakter, terwijl verwijderingsverzoeken (*referrals*) de vrijwillige keuze laat aan de internetbedrijven om content al dan niet te verwijderen in lijn met hun gebruikersvoorwaarden. Dit laatste instrument wordt nu gebruikt door de *Internet Referral Unit* (IRU) gevestigd bij de Nationale Politie en de EU IRU gevestigd bij Europol. Deze taak is overigens niet wettelijk vastgelegd.

Met het inzicht van nu wordt ervoor gekozen om alleen het instrument van verwijderingsbevelen in te zetten in lijn met de TOI-verordening. Dit houdt in dat er geen 'nationale kop' komt voor de optie van verwijderingsverzoeken en dat
10.2g deze niet in de uitvoeringswet wordt opgenomen. [redacted]

Toelichting

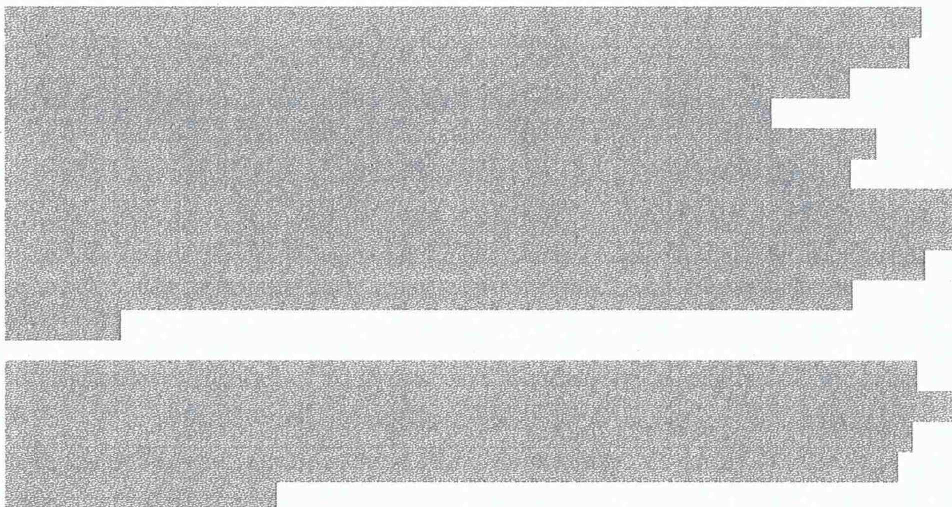
Argumentatie inzet van enkel verwijderingsbevelen

Het verwijderingsverzoek kan een aanvulling zijn op het verplichte instrumentarium uit de TOI-verordening. Met het inzicht van nu kan er nog geen beoordeling plaatsvinden. Daarom wordt in eerste instantie gekozen voor het uitvoeren van enkel de uit de TOI-verordening voortvloeiende verplichting van het uitvaardigen van verwijderingsbevelen.

Op de eerste plaats kent de TOI-verordening een dergelijk instrument van verwijderingsverzoeken niet. De aard van terroristische content is dusdanig ernstig dat er geen keuzevrijheid aan een private partij gelaten moet worden als het gaat om de vraag of en wanneer terroristische content ontoegankelijk gemaakt moet worden. Het ondersteunt de gedachte van de TOI-verordening om deze beoordeling aan een onafhankelijke autoriteit over te laten. Het verwijderingsbevel is, gelet op de ernst van terroristische content, een proportioneel, effectief en dwingend instrument om verspreiding van terroristische content online zo snel mogelijk tegen te gaan. Daarbij kent het verwijderingsbevel

rechtswaarborgen (bezwaar en beroepsmogelijkheden), die het verwijderingsverzoek niet kent (dit is immers op vrijwillige basis en daarmee afhankelijk van de gebruikersvoorwaarden van de internetprovider). Een (formeel) verwijderverzoek kan daardoor ook onduidelijkheid voor de praktijk tot gevolg hebben.

Op de tweede plaats heeft het ook om praktische redenen geen voorkeur. Het introduceren van een dergelijk instrument, zou een 'nationale kop' op de Uitvoeringswet van de TOI-verordening betreffen en daarmee het wetgevingsproces vrijwel zeker vertragen. Het verwijderverzoek volgt namelijk niet uit de verordening en is dan ook niet nodig om aan de verordening uitvoering te geven. Gelet op de korte implementatietermijn is dit onwenselijk.



10.2g [redacted]

[redacted]

T13



Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Dep. VERTROUWELIJK
Minister van Justitie en Veiligheid

Visie vooraf: DWJZ, DGP&V en DGRR

Directie Contraterrorisme

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Contactpersoon

[redacted]

10.2e

Datum
7 juli 2020

Ons kenmerk
x

nota

Verkenning Competente Autoriteit voor de uitvoering van de verordening Terroristische Content Online

Aanleiding
Nederland dient op grond van EU-verordening 'ter voorkoming van verspreiding van terroristische content online' (TCO-verordening) een competente autoriteit in te richten die uitvoering geeft aan de uit de TCO-verordening voortvloeiende maatregelen. Met het oog op de inrichting van een dergelijke autoriteit heeft de NCTV een verkenning uitgevoerd met een advies over de juridische grondslag en organisatievorm.

Advies

- Kennisnemen van deze nota;
- Instemmen met het advies om de competente autoriteit TCO op bestuursrechtelijke grondslag vorm te geven en daartoe een nieuw zelfstandig bestuursorgaan (ZBO) in te richten, zie bijgevoegde Verkenning voor onderbouwing van dit advies en het overzicht met verkende opties.
- Instemmen met voornemen om de bestuursrechtelijke aanpak van online kinderpornografische content (Kinderpornografische content) en online terroristische content (TCO) –voor zover mogelijk- onder te brengen in een gezamenlijke autoriteit.
- Instemmen met de agendering van een gesprek met staatssecretaris Knops (BZK) om overeenstemming te bereiken over de inrichting van een nieuwe ZBO (hierover wordt u separaat geïnformeerd).
- Kennisnemen van de nota met een toelichting op het rapport van de Adviesraad Internationale Vraagstukken 'Regulering van Online Content: naar een herijking van het Nederlandse internetbeleid'. Deze nota is relevant voor de discussie over de zelfstandigheid van de autoriteit.

Toelichting
Taken competente autoriteit (zie ook p.4 Verkenning)
De onderhandelingen over de verordening met als doel het voorkomen van de verspreiding van terroristische content online (COM 2018, 640 final) worden na verwachting voor het einde van 2020 afgerond onder het per 1 juli gestarte EU-voorzitterschap van Duitsland. Na akkoord is er een periode van 12 maanden voor implementatie van de verordening. De in te richten competente autoriteit (CA) monitort het internet op terroristische content en verstuurt verwijderbevelen (verplicht) en verwijderverzoeken (vrijwillig) aan internetbedrijven (hostingservice providers) die diensten aanbieden binnen de EU. Het verwijderbevel gaat vergezeld van een termijn van 1 uur waarbinnen de

betreffende content van het internet dient te zijn verwijderd. Daarnaast ontvangt de Nederlandse CA van CA's in andere EU lidstaten verwijderbevelen en -verzoeken, gericht aan in Nederland gevestigde internetbedrijven. Zij kan hier bezwaar tegen maken, maar dit bezwaar is niet bindend voor de uitvaardigende autoriteit. De Nederlandse CA kan daarnaast sancties en proactieve maatregelen opleggen aan in Nederland gevestigde hostingbedrijven.

Bestuursrechtelijke invulling (zie ook p.8 Verkenning)
De belangrijkste reden om te kiezen voor een bestuursrechtelijke grondslag boven een strafrechtelijke, is dat de verordening geen bestraffend, maar een reparatoir karakter heeft. Het doel van de verordening is het voorkomen van verspreiding van terroristische content op het internet en niet strafrechtelijke vervolging. Belangrijk is nog dat de bestuursrechtelijke grondslag meer passend is bij de toezichthoudende taken die de verordening voorschrijft, zoals het opleggen van proactieve maatregelen en toezicht houden op de maatregelen die internetbedrijven nemen tegen het verschijnen van terroristische content op hun platformen.

Nieuw op te richten zelfstandig bestuursorgaan (ZBO) (zie ook p.11 Verkenning)
In aanvulling daarop volgt uit de verkenning het advies om de CA vorm te geven als nieuw in te richten zelfstandig bestuursorgaan (ZBO). Deze keuze wordt met name gemotiveerd uit de wens om de CA op afstand te plaatsen van politieke besluitvorming. Dit vanwege het feit dat de taak van de autoriteit raakt aan de vrijheid van meningsuiting, en vanwege de kritische houding van Tweede Kamer jegens de verordening, juist vanwege de bescherming van grondrechten en de afwezigheid van een nationale rechtsgang tegen verwijderbevelen van buitenlandse CA's.

Het gaat hier in het bijzonder om de afweging of specifieke content als terroristisch dient te worden beoordeeld en dient te worden verwijderd (casuïstiek). Het lijkt passend dit niet onder directe ministeriele verantwoordelijkheid te plaatsen om de schijn van politieke beïnvloeding te voorkomen.

Samen optrekken met KiPo
Dit advies sluit aan bij de voorstellen voor een bestuursrechtelijke aanpak van online kinderpornografische content (KiPo) van DGRR. Eerder bent u geïnformeerd per nota over het voornemen om één Autoriteit in te richten voor zowel TCO als Kinderporno vanuit DRC[1]. In deze nota wordt u gevraagd daarmee in te stemmen. Zowel vanuit het oogpunt van de opbouw van kennis en expertise als vanuit efficiencyperspectief heeft het onderbrengen bij één gezamenlijke autoriteit de voorkeur. Dit schept ook het perspectief op ontwikkeling tot een volwaardige autoriteit die kan uitgroeien tot een geaccepteerde gesprekspartner voor de sector. Een autoriteit met twee taken verstrekt de argumentatie voor een nieuwe organisatie (boven het onderbrengen bij een bestaande organisatie). De

[1] Nota Bestuursrechtelijke aanpak kinderporno en Programmaplan voor 2020

Datum
7 juli 2020

Ons kenmerk
2968098

wetgevingstrajecten blijven wel afzonderlijk van elkaar lopen, gezien de strakke implementatietermijn van de TCO-verordening (na EU-akkoord 12 maanden[2]). In eerste instantie wordt de financiering afzonderlijk georganiseerd om op termijn te bezien welke financieringsvorm het best passend is bij de sturingsrelatie. Tot slot wordt één kwartiermaker aangetrokken die de autoriteit gezamenlijk organisatorisch vorm gaat geven.

Overleg met BZK over ZBO

Voor de oprichting van een ZBO is instemming vereist van het ministerie van BZK. Het kabinet voert een terughoudend beleid voor de oprichting van nieuwe ZBO's om wildgroei te voorkomen en vanwege de noodzaak van politieke verantwoordelijkheid bij de uitoefening van publieke taken. De uitoefening van taken door een zelfstandig bestuursorgaan geschiedt immers in beginsel buiten de ministeriële verantwoordelijkheid, en dat beïnvloedt de ruimte voor parlementaire controle op deze publieke taken.

10.2g [redacted] Wij adviseren u daarom om dit gesprek te vervolgen op politiek niveau met staatssecretaris Knops van BZK. Hierover zult u op korte termijn nader over worden geïnformeerd, waarbij een meer uitgebreide motivering voor de ZBO-keuze zal worden gedaan.

Terugvalopties (Zie ook p.9 t/m 11 Verkenning)

Op basis van de verkenning is onder partners een breed gedragen voorkeur voor een inrichting van een CA langs de lijnen zoals in de verkenning geschetst. Deze verkenning heeft de ondersteuning gekregen van de leden van het directeurenoverleg CTER[3].

Mocht het evenwel toch nodig zijn om alternatieven voor de inrichting van een ZBO te overwegen, dan kunnen de volgende opties worden verkend. Een optie is om de CA onder ministeriele verantwoordelijkheid te brengen en in te richten als een dienstonderdeel van het ministerie van J&V. Gezien de gewenste afstand tot de politiek-bestuurlijke besluitvorming heeft deze optie niet de voorkeur. Daarbij heeft u eerder in overleg met DRC aangegeven een dergelijk model voor kinderpornografische content niet wenselijk te vinden, maar wel mogelijkheden te zien voor het gezamenlijk onderbrengen van Kinderpornografische content en TCO in één autoriteit.

Andere mogelijkheden zijn het uitbreiden van de functie van de Internet Referral Unit bij de Nationale Politie of het opknippen van de taken van de CA tussen de

---

[2] Naar verwachting zal onder het Duits voorzitterschap een akkoord komen van de TCO-verordening.

[3] Leden van het directeurenoverleg CTER: IND, Politie (IRU), DGPenV, DGM, DGRR,DS&J, KMar, AIVD, BZK, Gemeente Den Haag, OM, BZ, SZW, AZ. DO vond plaats op 30 juni 2020

Autoriteit Telecom, die verwijderbevelen kan uitvaardigen en handhaven, en een partij die het internet kan monitoren, bijvoorbeeld de IRU. Deze twee terugvalopties zijn eveneens suboptimaal. Bij geen van beiden wordt voorzien in de gewenste afstand tot de politieke besluitvorming. Verder verhouden 1) de taken die voortvloeien uit de verordening zich moeilijk tot de kerntaak van de politie zoals neergelegd in de politiewet en 2) zou opknippen het werkproces (te) complex maken en slechts via een mandaatconstructie kunnen worden gerealiseerd (de AT valt onder EZK).

Vervolgstappen (zomer 2020)

Ervan uitgaande dat de onderhandelingen over de EU verordening in het najaar worden afgerond en de implementatietermijn van 12 maanden begin 2021, worden thans de volgende stappen gezet:

- Het uitwerken van een voorstel (business case) met een meer gedetailleerde beschrijving van de inrichting van de CA (taken, financiën, capaciteit, werkprocessen, governance etc.).
- Binnen de termijn van 12 maanden dient ook het nationale wetgevingstraject te zijn afgerond. Dit betekent dat voor het wetgevingsproces spoedprocedures (bij o.a. de Raad van State) nodig zijn. Voorbereidende werkzaamheden als het schrijven van een uitvoeringswet en de Memorie van Toelichting worden op dit moment samen met DWJZ opgestart.
- Wat de financiering betreft wordt totale kostenraming in kaart gebracht. Daarnaast wordt in overleg met DGP&V, de Nationale Politie en FEZ bezien welk deel van het reeds geoormerkte budget voor de Internet Referral Unit kan worden benut voor (gedeeltelijke) financiering van de autoriteit, indien er gekozen wordt voor een ZBO en ook de taken van de IRU daar worden ondergebracht. Het betreft hier zowel de onderbesteding over 2018, 2019 en 2020 waarmee mogelijk een deel van de implementatie kan worden bekostigd, als de structurele financiering na afloop van de implementatie termijn (de IRU ontvangt ca. 1,7 miljoen euro structureel). De verwachting is dat vrijvallende middelen niet voldoende zijn om de volledige kosten van de autoriteit te dekken.
- DRC en de NCTV zullen in de zomer de mogelijkheden verkennen voor de aanstelling van één gezamenlijke kwartiermaker, die ook een brug moet slaan tussen de business case Kinderpornografische content en de – nog uit te werken – operationalisatie TCO.

Afstemming

Leden van het directeurenoverleg CTER plus DWJZ, Agentschap Telecom, Inspectie Justitie en Veiligheid, EZK

Bijlage

- Bijlage 1 De verkenning voor een competente autoriteit voor de uitvoering van de verordening Terroristische Content Online.
- Bijlage 2 Overzicht verkende varianten competente autoriteit TCO
- Bijlage 3 Nota Adviesraad Internationale Vraagstukken 'Regulering van Online Content: naar een herijking van het Nederlandse internetbeleid'.

T14

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Verkenning
Een ***competente autoriteit*** *voor de uitvoering van de verordening* ***Terroristische Content Online***

Opstellers:	**Team CTER Online (NCTV)**
Opdrachtgevers:	**Directeuren CTER (Directeurenoverleg DO)**
Datum:	**7 juli 2020**
Status:	**Concept**

Inhoudsopgave

1 Voorstel verordening Terroristische Content Online

1.1 Aanleiding en inleiding

Recente terroristische aanslagen hebben aangetoond dat terroristen het internet misbruiken om nieuwe aanwas te verwerven, voorbereidende en faciliterende activiteiten te ontplooien en om angst onder het publiek aan te wakkeren. Een voorbeeld waarvan blijkt dat terroristische content inspirerend kan werken op zogenoemde 'lone actors' is de aanslag in Christchurch in Nieuw-Zeeland.[1] Terroristische content wordt online gedeeld via hosting service providers (HSP's). Naast deze invloed op individuen en de samenleving in bredere zin, heeft TCO ook negatieve gevolgen voor HSP's zelf (o.a. reputatieschade).

Tegen deze achtergrond heeft de Europese Commissie in september 2018 een voorstel gedaan, genaamd 'Voorstel voor een verordening van het Europees Parlement en de Raad ter voorkoming van de verspreiding van terroristische online-inhoud.[2]'.

De verordening eist dat iedere lidstaat een competente autoriteit opricht of aanwijst. Deze competente autoriteit gaat uitvoering geven aan de verplichte bepalingen die uit de verordening voortvloeien. De belangrijkste taak wordt het uitvaardigen van verwijderbevelen van terroristische content online en het opvolging geven aan de termijn van 1 uur waarbinnen deze content door de HSP dient te zijn verwijderd.

Hoewel nog niet duidelijk is wanneer de verordening definitief wordt vastgesteld, is het raadzaam om zoveel als mogelijk al voor de afronding van de definitieve besluitvorming van start te gaan met de (voorbereiding) van de implementatie. De belangrijkste overweging hiervoor is dat de verordening lidstaten een korte periode van 12 maanden geeft voor implementatie. Dit betekent onder meer dat voor het wetgevingstraject spoedprocedures in gang moeten worden gezet. Daarnaast dient de competente autoriteit te worden ingericht, zodat deze ook daadwerkelijk operationeel is na afloop van deze 12 maanden. Als Nederland de implementatietermijn overschrijdt, riskeert het een inbreukprocedure van Europese Commissie, inclusief hoge boetes.[3] Bij afronding van deze verkenning (mei 2020), is de verwachting dat de verordening kort na de zomer van 2020 zal worden vastgesteld.

Met het oog op de implementatie heeft de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) een verkenning uitgevoerd om te beoordelen op welke juridische grondslag de competente autoriteit in Nederland dient te worden gestoeld (bestuursrechtelijke of strafrechtelijk) en of voor de competente autoriteit een nieuwe organisatie dient te worden ingericht, of dat zij bij een bestaande organisatie kan worden ondergebracht. Deze verkenning is tot stand gekomen op basis van gesprekken met de partners: Analyse/NCTV, Juridische Zaken/NCTV, Directie Juridische Zaken en Wetgeving/ DWJZ, Programma Nederland Digitaal Veilig/NCTV, AIVD, OM, politie, DG Politie en Veiligheidsregio's, EZK, Agentschap Telecom, Directie Rechtshandhaving en Criminaliteitsbestrijding /DGRR, Facebook, Google en NL Digital.

Om tot een onderbouwd voorstel te komen voor de juridische grondslag en organisatievorm zijn verschillende scenario's besproken met partners en stakeholders. De besproken scenario's hebben geleid tot het advies om de competente autoriteit op bestuursrechtelijke basis in te richten in de vorm van een nieuw Zelfstandig Bestuursorgaan (ZBO). Hiervoor is instemming nodig van het ministerie van Binnenlandse Zaken, dat verantwoordelijke is voor het stelsel van ZBO's.

In dit document wordt nadere toelichting gegeven op het voorstel voor de TCO-verordening (hoofdstuk 1), de context waarin de competente autoriteit wordt opgericht (hoofdstuk 2), de keuze voor de bestuursrechtelijke uitvoering (hoofdstuk 3) en worden de afwegingen beschreven die hebben geleid tot de keuze voor een ZBO (hoofdstuk 4). Tot slot worden in hoofdstuk 5 de conclusie gedeeld en de vervolgstappen aangegeven.

---

[1] Rapport Dreigingsbeeld Terrorisme Nederland (DTN 50)

[2] Voorstel voor een VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD ter voorkoming van de verspreiding van terroristische online-inhoud Een bijdrage van de Europese Commissie aan de bijeenkomst van de EU-leiders in Salzburg op 19-20 september 2018. COM/2018/640 final

[3] Boetes beginnen bij 2.940.000 miljoen zonder plafond (in 2019).

1.2 Verplichtingen TCO-verordening en taken competente autoriteit

Verwacht wordt dat de EU-onderhandelingen over de verordening ter voorkoming van de verspreiding van terroristische inhoud rond de zomer van 2020 worden afgerond. Voor de implementatie van deze verordening dient Nederland binnen 12 maanden na afronding van de onderhandelingen een competente autoriteit in te richten die het internet monitort op terroristische content en verwijderbevelen (verplicht) en verwijderverzoeken (vrijwillig) aan in Nederland gevestigde internetbedrijven (hosting service providers) verstuurt. Daarbij wordt van de competente autoriteit een oordeel gevraagd over ontvangen verwijderbevelen en - verzoeken vanuit andere EU-lidstaten aan Nederlandse internetbedrijven.

Dit alles heeft tot doel het internet op te schonen van terroristische uitingen Het gaat dus niet om (een vorm van) strafrechtelijke vervolging. De hieronder beschreven taken en verplichtingen zijn gebaseerd op dit voorstel en de huidige staat van de onderhandelingen. Ook als zijn de onderhandelingen nog niet afgerond, er bestaat inmiddels een goed beeld van de eisen die aan de toekomstige competente autoriteit worden, wel kan dit beeld op een beperkt aantal specifieke onderdelen in de laatste onderhandelingsfase nog aan verandering onderhevig zijn.

De definitie van terroristische content in de verordening bepaalt mede de reikwijdte van het voorstel en sluit aan bij de eerdere definitie van terrorisme zoals geformuleerd in de CT-Richtlijn 2017/541. In het voorstel van de Europese Commissie wordt de volgende definitie gehanteerd van terroristische content:

'terrorist content' means one or more of the following information inciting or advocating, including by glorifying, the commission of terrorist offences, thereby causing a danger that such acts be committed; encouraging the contribution to terrorist offences; promoting the activities of a terrorist group, in particular by encouraging the participation in or support to a terrorist group within the meaning of Article 2(3) of Directive (EU) 2017/541; and instructing on methods or techniques for the purpose of committing terrorist offences.

De verordening eist dat iedere EU-lidstaat een competente autoriteit opricht of aanwijst. Deze competente autoriteit gaat uitvoering geven aan de verplichte taken die uit de verordening voortvloeien. Onderstaande verplichtingen komen voort uit de meest fundamentele taken en bevoegdheden die geregeld zijn in de verordening. Alle verplichtingen (waarop sancties getroffen kunnen worden) zijn genoemd in de artikelen: 3 t/m 11, 13, 14 en 16.

De meest fundamentele onderdelen zijn:

- Het uitvaardigen van verwijderbevelen
- Het uitvaardigen van verwijderverzoeken
- Het opleggen van specifieke maatregelen
- Handhaven op ontvangen en uitgevaardigde verwijderbevelen door andere lidstaten
- Opleggen van sancties
- Rapporteren aan Europese Commissie
- Opvolging geven aan consultatieprocedure bij ontvangen verwijderbevelen of verzoeken-.

1) Verwijderbevelen (verplicht karakter): door de verordening kan straks iedere EU-lidstaat een grensoverschrijdend verwijderbevel uitvaardigen aan een HSP die in de EU diensten aanbiedt. Iedere lidstaat is verplicht om één of meerdere competente autoriteiten aan te wijzen die hier invulling aan kan/kunnen geven.

Over de precieze invulling van de procedure rond grensoverschrijdende verwijderbevelen wordt nog onderhandeld. De toekomstige praktijk kan afwijken van de in dit voorbeeld beschreven procedure. Van belang is dat o.a. de waarborg wordt ingebouwd dat informatie niet zonder meer wordt verwijderd, maar dat er onder andere nader overeen wordt gekomen welke gegevens bewaard dienen te worden ten behoeve van de opsporing- en vervolging of dat de afweging moet worden gemaakt of het al dan niet het opsporingsbelang schaadt.

2) Verwijderverzoeken (vrijwillig karakter): door de verordening kan straks iedere lidstaat – naast de verwijderbevelen- een grensoverschrijdend verwijderverzoek uitvaardigen aan HSP's waarvan haar diensten/content in de EU zichtbaar zijn. Deze bevoegdheid lijkt sterk op de referral taak van de Nederlandse IRU.

De keuze om in een specifieke casus een verwijderverzoek of een verwijderbevel te sturen, ligt binnen de bevoegdheid van de competente autoriteit. Om deze afweging te maken kan worden overwogen om een toetsingskader vast te stellen waarin prioriteit aan bepaalde content kan

worden gegeven die binnen de scope valt van de verordening. Ook kan dit toetsingskader dienen om de keuze te maken tussen het uitvaardigen van een verwijderverzoek of verwijderbevel.

3) Specifieke maatregelen: de verordening verplicht HSP's om specifieke maatregelen te treffen om de verspreiding van terroristische content tegen te gaan op hun eigen platform(en). De verordening laat het aan de HSP's om te bepalen welke maatregelen zij treffen. Mogelijke voorbeelden van maatregelen zijn het actief monitoren van de content die op de eigen platformen aanwezig is of een identificatieplicht alvorens een persoon of partij klant kan worden. Ook kan de competente autoriteit van het land waar de HSP is gevestigd, specifieke maatregelen opleggen. Wat voor soort specifieke maatregelen kan door de lidstaat zelf worden bepaald. Bij het opleggen van maatregelen dient altijd rekening te worden gehouden met proportionaliteit, financiële draagkracht en de mate waarin de platformen van HSP's worden misbruikt voor de verspreiding van terroristische content.

Verder verplicht de verordening HSP's om uiterlijk drie maanden na het ontvangen van een verwijderbevel te rapporteren aan de competente autoriteit over de getroffen specifieke maatregelen. Uiterlijk 6 maanden na afloop van een kalenderjaar dient de HSP te rapporteren over de acties die zij heeft ondernomen voor het tegengaan van de verspreiding van terroristische content.

Het bovenstaande vraagt van de competente autoriteit specialistische kennis over de werking van het internet, over de aard en verschijningsvorm van terroristische content en over het fenomeen terrorisme in bredere zin. De competente autoriteit moet een deskundige gesprekspartner zijn voor de HSP's en dient gemotiveerd te kunnen afwegen of en zo ja welke specifieke maatregelen moeten worden opgelegd.

4) Handhaving en sancties: Bij het niet voldoen aan verplichtingen uit de verordening, kunnen sancties worden opgelegd aan HSP's door de competente autoriteit van de EU-lidstaat waar de HSP is gevestigd. De verordening schrijft geen expliciete sancties voor, maar gaat impliciet uit van geldelijke boetes. Wel kan bij het niet systematisch opvolgen van verwijderbevelen, een geldboete worden opgelegd van 4% van de wereldwijde omzet. Jurisdictie ligt ook in dit geval bij de lidstaat waar de HSP is gevestigd. Gronden waarvoor sancties kunnen worden opgelegd zijn het niet opvolgen van verwijderbevelen, het niet implementeren van specifieke maatregelen, het niet beoordelen van ontvangen verzoeken en het niet delen van informatie over bewijs van terroristische misdrijven.

De verordening geeft criteria aan die in overweging moeten worden genomen bij het al dan niet opleggen van sancties:

- de aard, de ernst en de duur van de inbreuk;
- het opzettelijke of nalatige karakter van de inbreuk;
- eerdere overtredingen door de rechtspersoon of natuurlijke persoon die verantwoordelijk wordt gehouden;
- de financiële draagkracht van de aansprakelijk gestelde rechtspersoon of natuurlijke persoon;
- het niveau van samenwerking van de HSP's met de bevoegde autoriteiten.
- de aard en de omvang van de aanbieders van hostingdiensten, met name voor micro-ondernemingen of kleine ondernemingen in de zin van richtlijn 2003/361/EG van de Commissie.

Bovenstaande vraagt dat de competente autoriteit toezicht houdt en handhaaft. Hier dient de competente autoriteit juridisch onderlegd te zijn voor het opleggen van maatregelen, het afhandelen van beroep, en binnen de EU te kunnen opereren.

5) Rapporteren: Iedere competente autoriteit rapporteert jaarlijks aan de Europese Commissie over het aantal uitgevaardigde verwijderverzoeken, verwijderbevelen en gevoerde juridische procedures tegen HSP's die te maken hebben gehad met terroristische content.

6) Samenwerken: de verordening verplicht de competente autoriteiten in EU-lidstaten om elkaar te informeren, gezamenlijk te coördineren waar nodig en samen te werken in het licht van de verwijderverzoeken en-bevelen alsook de opgelegd sancties en de wijze van handhaving. Dit wordt de consultatieprocedure genoemd. Hoe deze consultatieprocedure er precies uit gaat zien en wat eronder valt is nog onderdeel van lopende onderhandelingen.

2 Context

De aangekondigde wetgeving staat niet op zichzelf. Voor de verdere op- en inrichting van de onder de TCO-verordening voorziene competente autoriteit is het belang om rekening te houden met de specifieke kenmerken van het Nederlandse landschap van Hosting Service Providers (HSP's) en recente nationale ontwikkelingen met betrekking tot handhaving van overheidswege bij onwenselijke uitingen op internet. Hieronder wordt achtereenvolgens aandacht besteed aan:

- de Hosting Service Providers (HSP's)
- Programma Aanpak Kinderporno van het Ministerie van Justitie en Veiligheid/DGRR (KiPo)
- de Internet Refferal Unit (IRU) bij de Nationale Politie

2.1 Hosting Service Providers

Europol geeft aan dat in 2017 circa 150 bedrijven in Europa zijn geïdentificeerd als hosters van terroristische content.[4] Het is nog niet bekend welke hiervan als 'bad hosters'[5] bestempeld moeten worden.

Nederland is een van de lidstaten met het grootste aantal HSP's in de EU. Hoewel het precieze aantal HSP's niet bekend is, wordt geschat dat in Nederland ongeveer 10.000 hostingbedrijven gevestigd zijn. Het merendeel hiervan is klein (circa drie personen, incl. de eigenaar). Daarnaast zijn er ongeveer 100 bedrijven die professioneler zijn ingericht. Deze bedrijven zijn vaak tussen 5 en 15 werknemers groot. Tot slotte is er een aantal hele grote bedrijven zoals Leaseweb, Nforce en AFAS.

De verordening heeft voor kleine bedrijven een grotere impact dan voor grote bedrijven. Zo geeft koepelorganisatie NL digital aan zorgen te hebben over de 1-uur-verwijdertermijn en de eis om continue bereikbaar te zijn (24 uur per dag, 7 dagen per week) met het oog op het kunnen ontvangen van en opvolging geven aan verwijderbevelen. Het ministerie van EZK vroeg in dit verband aandacht voor de nalevingskosten van de internetindustrie.

Met Facebook en Google is gesproken over de mogelijkheden om de kleine internetbedrijven te ondersteunen bij hun inspanningen om te voldoen aan de eisen die uit de verordening voortvloeien. Bezien wordt op welke wijze en in welke mate afstemming met de hostingsector kan plaatsvinden bij voorbereiding van de implementatie van de verordening. Hierbij zal ook EZK worden betrokken dat veel contact heeft met de hostingsector en daardoor kan helpen met in kaart brengen van de economische gevolgen.

In dit verband wordt opgemerkt dat EZK al betrokken is bij de herziening van de Europese E-commerce richtlijn, straks Digital Service Act (DSA) genaamd. De DSA zal raakvlakken hebben met andere verordeningen die gaan over internetcontent. EZK en de NCTV blijven hierover met elkaar in contact om te voorkomen dat er tegenstrijdige bepalingen worden opgenomen.

2.2 Aanpak Kinderporno (KiPo)

De minister van JenV heeft op 3 juli jl. de Kamer nader geïnformeerd over zijn voornemen om naast zelfregulering en het strafrecht, ook bestuursrechtelijk te willen optreden tegen de hosting van kinderporno (KiPo). Doel hiervan is het opschonen van het internet. In deze aanpak wordt aangekondigd dat bedrijven te maken zullen krijgen met een bestuursorgaan dat door het opleggen van een last onder dwangsom en een bestuurlijke boete kan afdwingen dat kinderporno na een melding tijdig wordt verwijderd.

Het verantwoordelijk beleidsonderdeel, de directie Rechtshandhaving en Criminaliteitsbestrijding (DRC) bereidt momenteel besluitvorming voor. Hiervoor is een business case uitgewerkt, waarin een voorkeur wordt geformuleerd voor een nieuw in te richten Zelfstandig Bestuursorgaan (ZBO). Uitgaande van het beleidskader ZBO's, zoals geformuleerd in de kaderwet adviescolleges, kan een ZBO voor de aanpak van KiPo worden gemotiveerd volgens de motieven die staan genoemd in de Memorie van Toelichting bij de Kaderwet: onafhankelijkheid, regel gebonden uitvoering en

[4] Meer dan de helft van deze bedrijven bieden "file storage" en "sharing services" aan. 20% van deze bedrijven biedt "online media sharing services" aan. Ongeveer 10% betreft "web hosting services". Ongeveer 10% betreft "social networking" en "discussion forums".

[5] Bad hosters zijn HSP's waarvan bekend is dat zij klanten hebben die illegale content op hun servers draaien, zoals kinderpornografische of terroristische content, maar nalatig zijn in het nemen van welke vorm van verantwoordelijkheid ook.

participatie. Onafhankelijkheid is van belang, omdat het bestuursorgaan voor de aanpak KiPo werkt op de scheidslijn van netwerk(infrastructuur) en content. Aangezien content direct raakt aan fundamentele vrijheden is het voor draagvlak en gezag van het bestuursorgaan belangrijk dat deze op afstand staat van de politiek en van de minister[6].

De voorgestelde bestuursrechtelijke aanpak van KiPo vertoont grote overeenkomsten met de aanpak van terroristische uitingen op internet, zoals gemotiveerd in deze verkenning. Tegen deze achtergrond wordt in de business case voor de aanpak van KiPo het perspectief geschetst van een bredere autoriteit internetveiligheid waarin naast de aanpak van KiPo, ook de aanpak van andere content op internet kan er worden ondergebracht, zoals terroristische content.

De besluitvorming over de bestuursrechtelijke aanpak van KiPo is nog niet afgerond. Momenteel vinden gezamenlijke gesprekken plaats van DRC en NCTV met het ministerie van BZK, dat verantwoordelijk is voor het stelsel van ZBO's. BZK stelt zich, in lijn met het huidige kabinetsbeleid, zeer terughoudend op ten aanzien van de inrichting van nieuwe ZBO's of het onderbrengen van nieuwe taken bij bestaande ZBO's. Een ZBO dient namelijk een uitzondering te zijn, wanneer andere (gangbaardere) vormen niet mogelijk of wenselijk zijn.

2.3 Internet Referral Unit (IRU)

Bij de Nationale Politie, Landelijke Eenheid (LE), is per 1 september 2017 een Internet Referral Unit (IRU) ingericht. De IRU komt voort uit het Actieprogramma Integrale aanpak Jihadisme (2014). De IRU richt zich op detectie en duiding van online jihadistische content, identificatie van producenten en verspreiders en melding van content die in aanmerking komt voor een verwijderverzoek (Notice and Take Action (NTA). Dit betekent dat wanneer de IRU terroristische content identificeert en duidt, zij vervolgens verwijderverzoeken opmaakt en verstuurt aan bedrijven. De IRU werkt samen met zusterdiensten in andere EU-lidstaten en Europol. Bepaalde verplichtingen uit de verordening lijken sterk op de taken die de IRU nu uitvoert.

In samenspraak met het Openbaar Ministerie is een kader vastgesteld om te kunnen duiden in welke gevallen NTA wordt toegepast. Als uitgangspunt voor NTA wordt door de IRU getoetst aan het wetboek van strafrecht. NTA wordt toegepast bij het vermoeden (uitings-)delicten waarop, zou sprake zijn van vervolging, minstens 4 jaar gevangenisstraf is gesteld, zoals opruiing en werven voor de gewapende strijd. Hiermee wordt aangesloten bij de nieuwe wet computercriminaliteit die op 1 maart 2019 in werking is getreden. Daar geldt dezelfde afbakening van misdrijven waarbij de officier van justitie een bevel tot ontoegankelijk making van gegevens kan geven.

Voor de uitvoering en borging van de taak van de IRU en deelname aan het programma Aanpak
online is sinds 2018 structureel financiering vrijgemaakt. [redacted]
10.2.g . De IRU maakt structureel
onderdeel uit van de formatie van Team OSINT (Open Source Intelligence) van de Nationale
10.2.g Politie. [redacted].

Onderzocht moet worden hoe de huidige taken, expertise en netwerken van de IRU van pas kunnen komen bij de opzet, implementatie en operationalisering van de competente autoriteit. Ook dient bezien te worden hoe de OSINT-werkzaamheden van de politie (primair gericht op opsporing en verzameling van intelligence) de werkzaamheden van de competente autoriteit kunnen versterken in de bestuursrechtelijke aanpak en vice versa. Een belangrijke overweging hierbij is dat de competente autoriteit, wanneer deze als nieuw bestuursorgaan wordt ingericht, (een deel van) de IRU-taken die thans bij de Nationale Politie zijn belegd, overneemt.

Verder bestaat bij de CT-partners de overtuiging dat effectievere bundeling van de kennis en ervaring van de verschillende organisaties die zich met schadelijke content bezighouden, kan bijdragen aan effectievere ondermijning van extremistische onlinebewegingen in Nederland. Tegen deze achtergrond zijn de NCTV, Politie, KMAR, AIVD en MIVD in 2018 het programma Aanpak Online Open Source Terrorisme (OSINT) gestart.

[6] Businesscase Autoriteit Kindermisbruik (september 2019)

3 Bestuursrechtelijke of strafrechtelijke uitvoering?

De TCO-verordening laat lidstaten de ruimte om te kiezen voor een bestuursrechtelijke, judiciële of strafrechtelijke competente autoriteit, of een combinatie van deze autoriteiten. De keuze voor de juridische grondslag bepaalt in hoge mate welke taken de competente autoriteit kan gaan uitvoeren en in welke vorm en waar de competente autoriteit kan worden ondergebracht.

Het advies is om in Nederland te kiezen voor een enkele bestuursrechtelijke autoriteit. Daarvoor is ten eerste relevant dat de verordening een reparatoir karakter heeft. De verordening heeft niet tot doel om diegenen die terroristische content produceren en op internet plaatsen op te sporen en te vervolgen; de verordening is er louter op gericht om online terroristisch content zo snel mogelijk ontoegankelijk te maken en dit zo nodig af te dwingen. De verwijderverzoeken en –bevelen worden daarom niet gericht tot diegene die terroristisch content produceren en op het internet plaatsen, maar tot aanbieders van hostingdiensten. De dienstverlening van deze aanbieders bestaat uit de opslag en doorgifte van gegevens die van een derde afkomstig zijn. De dienstverlening heeft een passief karakter: deze bedrijven hebben geen inhoudelijke betrokkenheid bij de gegevens die middels hun diensten worden verspreid. De bevoegdheden uit de verordening hebben in zoverre een reparatoir karakter, en zijn niet punitief van aard.

Bovendien zijn de taken uit de TCO-verordening te herleiden tot een vorm van toezicht op de naleving van wettelijke normen (die in de verordening zijn neergelegd), gecombineerd met handhavend optreden waar die naleving onvoldoende is. Dit is naar zijn aard een bevoegdheid die binnen het bestuursrecht wordt uitgeoefend. Het bestuursrechtelijk systeem, waar besluiten direct uitvoerbaar zijn en rechterlijke toetsing veelal achteraf plaatsvindt, sluit ook goed aan op het door de TCO-verordening beoogde model waarin de snelheid van verwijdering voorop staat.

Een aantal taken uit de verordening leent zich ook inhoudelijk minder goed voor uitvoering binnen het strafrecht of door een judiciële autoriteit. Dat geldt bijvoorbeeld voor de bevoegdheid om – in samenwerking met een HSP – te bezien of door de HSP getroffen specifieke maatregelen afdoende zijn, en om dergelijke maatregelen dwingend voor te schrijven waar dat niet het geval is. Dit leent zich minder goed voor uitoefening in het strafrecht, waar een sanctie doorgaans wordt opgelegd door de strafrechter, op vordering van het OM. Het figuur van een judiciële beslisautoriteit is in Nederland vrijwel onbekend.[7]

Ten slotte is de keuze voor een enkele autoriteit ingegeven uit organisatorisch oogpunt: omdat de verordening sterk de nadruk legt op samenwerking met HSP's en andere competente autoriteiten, is het uit organisatorisch oogpunt het best werkbaar alle taken onder te brengen in één nationaal bestuursorgaan. Dat is ook in het belang van de markt, die daarmee één aanspreekpunt heeft.

De keuze voor een bestuursrechtelijke uitvoering wordt ondersteund door het OM en de politie. De politie/ het OM menen de capaciteit beter in te kunnen zetten ten behoeve van de opsporing en vervolging van strafbare feiten dan ten behoeve van onwenselijke content. Bovendien gaat deze verordening het tot doel het internet op te schonen van terroristische uitingen Het gaat dus niet om (een vorm van) strafrechtelijke vervolging, en daarmee leent het bestuursrecht hier beter voor.

[7] Daarop lijkt nog het meest de rechter-commissaris uit het strafrecht.

4 Oprichting Competente Autoriteit

In de gesprekken met partners en stakeholders is een aantal mogelijkheden besproken voor de inrichting van een competente autoriteit in Nederland. Het betreft hier drie varianten met directe ministeriele verantwoordelijkheid en twee waarbij de ministeriele verantwoordelijkheid enigszins is ingeperkt:

- De taken onderbrengen bij de Nationale Politie (IRU)
- De taken onderbrengen bij een agentschap (Agentschap Telecom)
- De taken onderbrengen bij de inspectie van J&V.
- Een bestaande ZBO (Autoriteit Consument en Markt).
- Een nieuw in te richten ZBO.

Om een keuze te kunnen maken tussen de verschillende opties en om te komen tot een advies, is een aantal uitgangspunten geformuleerd waar de organisatie(vorm) aan moet voldoen. Deze uitgangspunten zijn:

- De CA dient binnen 12 maanden te worden op- en/of ingericht.
- De autoriteit dient onafhankelijk te zijn in de keuzes die worden gemaakt.
- De taken van de competente autoriteit worden ondergebracht bij één bestuursorgaan
- De competente autoriteit dient een bestuursrechtelijk mandaat te krijgen.
- Er wordt toegewerkt naar een duidelijke en logische eigenaar-opdrachtgevers-en opdrachtnemersrol volgens de sturingsdriehoek van het ministerie van Justitie en Veiligheid.

Het zwaarstwegende uitgangspunt is de onafhankelijkheid van competente autoriteit. Deze komt tot uitdrukking in de manier waarop de ministeriele verantwoordelijkheid is geregeld. De onafhankelijkheid is van belang omdat de verwijdering van TCO kan raken aan fundamentele vrijheden (zoals artikel 7 van de Grondwet; vrijheid van meningsuiting en verbod op censuur).

4.1 Competente autoriteit onder ministeriele verantwoordelijkheid

4.1.1 De politie/IRU

Gelet op het feit dat de IRU al taken uitvoert die vergelijkbaar zijn met de taken die voortvloeien uit de verordening, is voorstelbaar dat zij de rol van competente autoriteit op zich neemt. Dit lijkt ook, mede in het licht van de korte implementatietermijn, praktische voordelen te hebben. Er kan immers worden aangehaakt bij een reeds bestaande organisatie, al zal ook deze extra capaciteit en expertise nodig hebben voor de uitvoering van deze taken.

Tegen een dergelijke oplossing voor de inrichting van de competente autoriteit bestaat evenwel een aantal zwaarwegende bezwaren. [redacted]

10.2.g & 11.1

10.2.g & 11.1 [redacted]

10.2.g & 11.1 [redacted]

[redacted]

10.2g & 11.1 [redacted]

10.2g + 11.1 [redacted]

Een nieuw in te richten autoriteit op basis van de EU-verordening zou de mogelijkheid scheppen de taken die samenhangen met de verwijdering van terroristische content buiten de politie te plaatsen. Dit zou betekenen dat zowel de taken die zijn gericht op vrijwillige verwijdering als de taken die zien op verplichte verwijdering (inclusief bestuursrechtelijke handhaving voor beide) bij één nieuwe organisatie worden belegd. Deze oplossing behoudt het voordeel van efficiency en expertise opbouw, maar is te verkiezen vanuit het perspectief van verantwoordelijkheden en de inrichting van het politiebestel.

4.1.2 Agentschap Telecom

Agentschap Telecom (AT) is een onderdeel van het ministerie van Economische Zaken en Klimaat. Het agentschap is toezichthouder en uitvoerder van een groot aantal taken rondom telecommunicatie en de (digitale) diensten die daarmee geleverd worden. Beheer van het Nederlandse radiospectrum is een belangrijk onderdeel daarvan en daarnaast houdt AT ook toezicht op continuïteit van openbare telecomdiensten, digitale weerbaarheid van een aantal vitale en aangewezen sectoren en vertrouwensdiensten. Ook HSP's vallen (deels) onder het toezicht van AT.

Het AT voert ook voor andere ministeries toezicht uit (bijvoorbeeld Kijkwijzer wetgeving voor het ministerie van JenV en Wet Digitale Overheid voor het ministerie van BZK). Het AT geeft aan een deel van de rol als (evt. met KiPo gemeenschappelijke) competente autoriteit op zich te kunnen nemen, voor zover dit zou gaan over het toezien op de opvolging van gegeven verwijderingsbevelen door HSPs. Een vergelijkbaar construct bestaat ook voor het bevoegd aftappen. het AT handhaaft daar de voorziening die getroffen moet zijn om telecomdata af te tappen, de uitvoering van taplasten ligt niet bij AT. AT richt zich op een veilige en betrouwbare (digitale) infrastructuur. De oordeelsvorming over de aanwezige content bij digitale media ligt in Nederland primair bij het OM en de Nationale Politie.

Tegen deze achtergrond, wordt door AT de mogelijkheid geopperd om het proces van de competente autoriteit op te knippen tussen een partij die de terroristische content op het internet beoordeelt (zoals bijvoorbeeld de IRU) en een tweede partij die het verwijderbevel uitstuurt en handhaaft (zoals bijvoorbeeld AT). AT gaf aan dat zij vanuit hun huidige taak en expertise en bekendheid met HSP's, in staat zijn verwijderbevelen uit te vaardigen en specifieke maatregelen op te leggen. Hierbij is de content reeds als terroristisch beoordeeld door een andere partij. AT heeft echter wel veel kennis van de hostingbranche en de technische (on)mogelijkheden voor bedrijven als het gaat om specifieke maatregelen en verwijtbaarheid (i.r.t. sancties).

Dit model heeft nadelen omdat AT geen uitvoering kan geven aan de gehele TCO-verordening. Het samenbrengen van de beoordeling en uitvoering zorgt voor een vloeiende samenwerking en is
10.2g + 11.11 voor de branche ook duidelijker. Verder zal, in dit model, dienen te worden bezien of bijvoorbeeld de IRU een rol kan spelen in het beoordelen van content. [redacted]

Daarnaast is AT een agentschap van het ministerie van EZK. De staatssecretaris van EZK is verantwoordelijk voor AT dat als agentschap direct onder de ministeriële verantwoordelijkheid valt. Hiermee staat het niet op afstand, zoals een ZBO. De minister van Justitie en Veiligheid zou middels een mandaatconstructie de verantwoordelijkheid kunnen dragen voor dat deel van de taken van AT dat betrekking heeft op uitvoering van de verordening en daartoe ook aanwijzingen kunnen geven aan bij AT werkzame ambtenaren.

4.1.4 Inspectie van Justitie en Veiligheid

De Inspectie van JenV houdt toezicht op de kwaliteit van de taakuitvoering door organisaties werkzaam op het terrein van justitie en veiligheid (JenV). Daarbij onderzoekt de Inspectie of deze organisaties zich houden aan de wet- en regelgeving om vervolgens leerpunten te benoemen, zo nodig aanbevelingen te formuleren en door te interveniëren.

De uitvoering van wet- en regelgeving van de TCO-verordening past niet bij bovenstaande kerntaak die de Inspectie verricht. De Inspectie houdt toezicht op andere organisaties op het terrein van JenV. De nieuwe competente autoriteit gaat over uitvoering van wet- en regelgeving. Daarnaast is de inspectie niet toegerust op en ontbreekt ervaring bij het uitvoeren van de voorgestelde taken. De uitvoering van de verplichtingen uit de verordening zullen een flinke investering vergen.

Een ander belangrijk argument waardoor het niet wenselijk wordt geacht om de competente autoriteit onder te brengen bij de Inspectie is, dat sommige verplichtingen op gespannen voet staan met de kerntaken van de Inspectie. Bijvoorbeeld bij een verwijderbevel/verwijderverzoek. Hier zal de Nederlandse competente autoriteit moeten afwegen of er bezwaren zijn in het verwijderen van content en of de verwijdering wenselijk is. Hierbij kunnen lopende opsporings- en/of inlichtingenonderzoeken in Nederland worden doorkruist. Om te voorkomen dat dit plaatsvindt zal de competente autoriteit moeten samenwerken met onder meer de Politie. Nu de Inspectie ook toezichthouder op de taakuitvoering van de Politie is, is vermenging van de toezichthoudende taak met deze uitvoerende taak zeer onwenselijk.

Bovenstaande punt laat ook zien dat als de Inspectie wordt aangewezen als competente autoriteit de onafhankelijkheid in het geding komt. Tot slot komt de onafhankelijkheid verder in het nauw doordat de Aanwijzingen Rijksinspecties - waarin de onafhankelijkheid van de Inspectie van JenV, is gewaarborgd - zien op de uitoefening van toezichtstaken die de Inspectie uitvoert. Uitvoeringstaken, waaronder de voorgestelde taken in het kader van de TCO-verordening, vallen daar niet onder.

Concluderend wordt het als onwenselijk gezien om de competente autoriteit onder te brengen bij de Inspectie van Justitie en Veiligheid vanwege het niet kunnen waarborgen van de onafhankelijkheid en dat de uitvoering van de TCO-verordening op gespannen voet staat met de kerntaak van de Inspectie.

4.2 Competente autoriteit met beperkte ministeriele verantwoordelijkheid

4.2.1. Waarom een ZBO?

Zoals aangegeven wordt voor de bestuursrechtelijke aanpak kinderporno van DRC, eveneens de oprichting van een ZBO overwogen. De overwegingen hiervoor staan beschreven in de business case autoriteit kindermisbruik uit september 2019. Ook deze bestuursrechtelijke aanpak ziet toe op het schonen van het internet van ongewenste content. Daarmee zijn de overwegingen en opgenomen maatregelen die worden gemaakt bij de aanpak kinderporno, gelijk aan die van de overwegingen voor de uitvoering van de TCO-verordening. In de businesscase van DRC wordt toegelicht dat de Kaderwet ZBO drie instellingscriteria kent voor het instellen van een ZBO. Een ZBO kan uitsluitend worden ingesteld indien:

a. Er behoefte is aan onafhankelijke oordeelsvorming op grond van specifieke deskundigheid;
b. Er sprake is van strikt regel gebonden uitvoering in een groot aantal individuele gevallen;
c. Participatie van maatschappelijke organisaties in verband met de aard van de betrokken bestuurstaak bijzonder aangewezen moet worden geacht.

Zoals in het geval van de aanpak KiPo gelden deze drie criteria ook voor de competente autoriteit ter voorkoming van de verspreiding van terroristische online-content. Verreweg het belangrijkste criterium, in het geval van de competente autoriteit, is het onafhankelijkheidscriterium. Hiermee wordt bedoeld de onafhankelijkheid ten opzichte van de politiek, zoals nog eens onderstreept in de Kamerbrief van 16 mei 2014[8]. Deze onafhankelijkheid komt tot uitdrukking in het feit dat ZBO's niet hiërarchisch ondergeschikt zijn aan de Minister en dat de ministeriële verantwoordelijkheid ten aanzien van ZBO's is ingeperkt.

Het onafhankelijkheidscriterium in het geval van de verordening ter voorkoming van de verspreiding van terroristische online content heeft een bijzonder zwaar gewicht omdat het bij het schonen van het internet gaat om maatregelen die kunnen raken aan fundamentele rechten, zoals

[8] Kamerbrief Zelfstandige Bestuursorganen, 16 mei 2014, vergaderjaar 2013-2014, 25268 nr. 83

de vrijheid van meningsuiting. Telkens wanneer sprake is van een bevel of verzoek tot verwijdering van terroristische content, dient zorgvuldig getoetst te worden aan deze rechten. Daarom is een deskundige en zo onafhankelijk mogelijke oordeelsvorming, los van de (schijn) van politiek besluitvorming, van groot belang. Hierbij wordt tevens in overweging genomen dat de Tweede Kamer zich kritisch opstelt ten opzichte van de verordening en bij de minister heeft aangedrongen op voldoende juridische waarborgen. Op last van de Tweede Kamer heeft deze nadrukkelijk bij andere EU-lidstaten en de Europese Commissie aandacht voor deze waarborgen gevraagd tijdens de onderhandelingen over de verordening. Dit laatste is een belangrijke aanvullende overweging, gelet op het feit dat de drie instellingscriteria (die in de Kaderwet ZBO's zijn benoemd) noodzakelijke zijn, maar niet-voldoende voorwaarden voor een ZBO-status. Er is dus altijd een aanvullende motivering nodig, bijvoorbeeld dat internationale regelgeving vereist dat onafhankelijkheid vorm krijgt door zelfstandigheid, zoals ook beschreven in de Kamerbrief van 16 mei 2014. Een nadeel van de zelfstandigheid van een ZBO is dat door diezelfde beperkte ministeriële verantwoordelijkheid de minister niet sturend kan optreden, ook niet als dit noodzakelijk blijkt Dit lijkt evenwel niet op te wegen tegen het belang van onafhankelijkheid van de competente autoriteit.

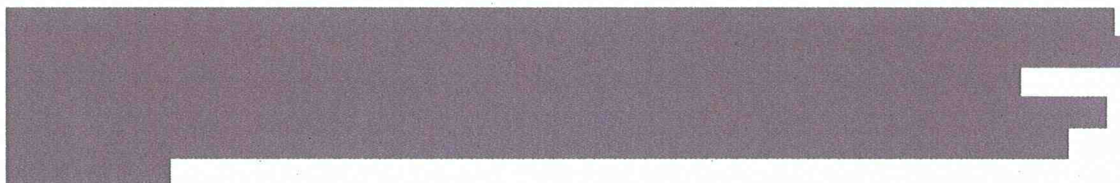
De afstand tot de minister is een belangrijk voordeel van een ZBO boven alternatieve organisatievormen met een bestuursrechtelijke grondslag, zoals het onderbrengen van de competente autoriteit bij het Ministerie van Justitie en Veiligheid zelf, een agentschap of de uitbreiding van het takenpakket van de IRU bij de Nationale politie.

De andere twee criteria uit de Kaderwet op ZBO's zijn net als in het geval van de bestuursrechtelijke aanpak KiPo, ook van toepassing op de competente autoriteit. Het betreft niet alleen de uitvoering van specifieke regelgeving met het oog op de borging van een breed maatschappelijk belang, die voor de gehele Nederlandse sector van hosting service providers van toepassing is en deels - in geval van verwijderbevelen en -verzoeken op case-by-case basis dient te worden toegepast (criterium 2). Daar komt bij dat de introductie van zogenaamde specifieke maatregelen en de ontwikkeling van het toezicht daarop, nauwe samenwerking vereisen met de sector en zijn vertegenwoordigers (criterium 3). Hierbij geldt dat voor de sector, zoals ook in de business case KiPo herkend wordt, dat politieke onafhankelijkheid, voorspelbaarheid en reguleringszekerheid van groot belang zijn en bijdragen aan wederzijds vertrouwen tussen de sector en de competente autoriteit. Dit komt de effectiviteit van de maatregelen ten goede.

4.2.2. Bestaande ZBO – Autoriteit Consument en Markt

Wanneer ervoor wordt gekozen de competente autoriteit onder te brengen in een ZBO, kan dit door de taken te beleggen bij een bestaande ZBO of door hiervoor een nieuwe ZBO in te richten. Voor de eerste optie is door DGRR verkend in hoeverre de Autoriteit Consument en Markt de uit de verordening voortvloeiende taken zou kunnen invullen. Andere ZBO's zijn op voorhand niet geschikt bevonden om de competente autoriteit onder te brengen.

De ACM leek een goede partner - ondanks haar positionering onder het ministerie van EZK - omdat zij als markttoezichthoudererervaring heef met het houden van toezicht op de naleving van Europese regelgeving, zoals bijvoorbeeld bij de EU e-commerce richtlijn.

10.2g  [redacted]

Hier is de conclusie getrokken dat de ACM geen voorkeur geniet bij het onderbrengen van de competente autoriteit, gezien haar rol en taakopvatting als toezichthouder. De taken die voortvloeien uit de verordening zijn wezensvreemd aan haar kerntaken.

4.2.3. Nieuw in te richten ZBO

Om bovenstaande redenen alleen al heeft de inrichting van een nieuwe ZBO sterk de voorkeur.

Daarbij komt dat de keuze voor een nieuwe ZBO ook een belangrijk intrinsiek voordeel heeft voor de (door)ontwikkeling van toezicht op ongewenste content op internet. De inrichting van een nieuw bestuursorgaan zou een basis creëren voor een meer volwaardige toezichthouder op

[9] De autoriteit Consument en Markt (ACM) houdt toezicht op mededinging, aantal specifieke sectoren (bijv. post, telecom en zorg) en de bescherming van consumenten

ongewenste uitingen op internet. Dit is nu al relevant, zoals de parallelle discussie over de bestuursrechtelijke aanpak van online kinderporno laat zien, waarbij eveneens de inrichting van een ZBO wordt overwogen. Met de keuze voor een nieuw in te richten bestuursorgaan wordt ruimte gecreëerd om gezamenlijk op te trekken en te overwegen om het tegengaan van zowel online kinderporno als terroristische uitingen op internet onder te brengen in één organisatie.

Verder kan bij een nieuwe ZBO een gedegen eigenaar – opdrachtgever – opdrachtnemer relatie worden opgezet. De ZBO zou geheel zelfstandig haar besluiten kunnen nemen en, in de toekomst, de contacten met het bedrijfsleven kunnen onderhouden over bijvoorbeeld nieuwe technologische middelen. Het ministerie van Justitie en Veiligheid zou in gezamenlijkheid met de ZBO langer termijn doelstellingen kunnen formuleren.

4.2.4. Beleidskader ZBO's

Hoewel de oprichting van een nieuwe ZBO (net zoals voor het onderbrengen van nieuwe taken bij een bestaande ZBO) de voorkeur geniet, is hiervoor instemming nodig van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK). BZK is verantwoordelijk voor het kabinetsbeleid inzake het stelsel van ZBO´s. Belangrijk kenmerk van dit beleid is de terughoudendheid bij het toekennen van taken aan (nieuwe) ZBO's. Deze terughoudendheid is terug te voeren op de noodzaak van het doorvoeren van transparante verantwoordelijkheid bij de inrichting van publieke taken. Het beleggen van taken bij ZBO's kan wenselijk zijn, maar kent per definitie enige "transparantieschade" als het gaat om parlementaire verantwoording. Dit betekent dat publieke taken bij een voorkeur onder directe ministeriele verantwoordelijkheid worden gebracht

Het vigerende kabinetsbeleid inzake ZBO's betekent dat de oprichting van nieuwe ZBO's al enige jaren een uitzondering is. Onmogelijk is dit evenwel niet. In de periode 2014-2019 zijn zes nieuwe ZBO's opgericht. In het geval van kinderpornografische én terroristische uitingen is een uitzonderingsgrond aanwezig. Vanwege de precaire balans tussen het fundamentele recht van vrijheid van meningsuiting en het belang van een 'schoon' internet, zou het toezicht juist niet onder directe ministeriele verantwoordelijkheid moeten worden gebracht. De minister van J&V heeft in het dossier KiPo de voorkeur uitgesproken voor de inrichting van een ZBO, rekening houdend met de mogelijkheid van uitbreiding met de taak van de competente autoriteit. Definitieve besluitvorming heeft evenwel ook in het geval van KiPo nog niet plaatsgevonden. Gezamenlijk met KiPo dient nader met BZK te worden overlegd.

5 Conclusie en vervolgstappen

Conclusie

Met het oog op de implementatie, is in deze verkenning gemotiveerd op welke juridische grondslag de competente autoriteit in Nederland moet worden gestoeld (bestuursrechtelijke of strafrechtelijk) en of voor de competente autoriteit een nieuwe organisatie dient te worden ingericht, of dat zij bij een bestaande organisatie kan worden ondergebracht. Op basis van het de overwegingen in met name hoofdstuk 3 en 4, wordt geadviseerd om de competente autoriteit op bestuurlijke grondslag in te richten en dit vorm te geven door het oprichten van een nieuw zelfstandig bestuursorgaan (ZBO).

Voornaamste reden om voor een bestuursrechtelijke vorm te kiezen is omdat het doel van de verordening het voorkomen van verspreiding van terroristische content op het internet is en niet-strafrechtelijke vervolging. Andere belangrijke voorwaarde voor oprichting van de competente autoriteit is dat het vrij moet zijn van (de schijn van) politieke beïnvloeding/besluitvorming. Daarom wordt ten zeerste aangeraden om te kiezen voor een zelfstandig bestuursorgaan. Dit advies wordt in deze verkenning gegeven, omdat deze vorm van op- en inrichting van de competente autoriteit de meest gunstige randvoorwaarden biedt voor de uitvoering van de taken die uit de voortvloeien, alsmede voor het contact met de hostingsector en de opbouw van kennis en expertise. Tegelijkertijd creëert zij voldoende waarborgen creëert voor de gewenste onafhankelijkheid. De andere geschetste opties scoren op beide punten beduidend minder.

Vervolgstappen

Als aangegeven is het van belang om tijdig met de implementatie te starten vanwege de korte implementatietermijn (12 maanden) die de verordening lidstaten geeft en het risico van een inbreukprocedure wanneer niet aan deze termijn wordt voldaan. Dit betekent dat er op het moment dat de formele implementatietermijn start, en bij voorkeur al daarvoor, een beeld moet bestaan van de invulling van een aantal overige randvoorwaarden voor de inrichting van de autoriteit, zoals financiën, de feitelijke organisatie-inrichting en de relatie met de aanpak KiPo.

Met het oog hierop zal de NCTV een nadere business case uit te werken, waarin onder meer zal worden geschetst welke taken de competente autoriteit zal moeten uitvoeren, welke kennis en expertise zij hiervoor in huis dient te hebben, hoeveel capaciteit hiervoor nodig is (fte) en welke kosten hier naar verwachting mee gemoeid zullen zijn. Ook zal een beeld worden gegeven van de belangrijkste werkprocessen, inclusief het doen van verwijderbevelen en verzoeken, alsmede van de aansturings- of governancestructuur.

Wat de financiering betreft, zal naast het in beeld brengen van een totale kostenraming, in overleg met DGP&V en de Nationale Politie worden bezien wel deel van het reeds geoormerkte budget over de periode 2018-2022 voor de Internet Referral Unit, kan worden benut voor (gedeeltelijke) financiering van de autoriteit. De Nationale Politie ontvangt sinds 2018 structureel jaarlijks ruim financiering euro voor de IRU uit de door het huidige kabinet toegekende intensiveringsmiddelen voor contra-terrorisme. Deze middelen zijn onder coördinatie van de NCTV in overleg met de CT-partners verdeelt over een aantal prioritaire CT-taken, waaronder de aanpak van terroristische uitingen op internet. Wanneer het advies uit de onderhavige verkenning wordt gevolgd en de competente autoriteit inderdaad de referral taak van de IRU overneemt, dan ligt het in de rede dat ook (een deel van) het reeds voor deze taak geoormerkte budget bij de Nationale Politie voor de (implementatie) van de competente autoriteit wordt aangewend. Eventuele aanwending van IRU-middelen strekt zich uit over zowel de onderbesteding over 2018, 2019 en 2020, als de begrote middelen voor 2020 en 2021 en verder.

Gelet op de mogelijkheid dat nog in 2020 een start dient te worden gemaakt met de implementatie, wordt ernaar gestreefd zowel de business case als het voorstel voor aanwending van de IRU-middelen aan het einde van de zomer 2020 gereed te hebben. Dit biedt de gelegenheid om nog dit jaar financiële mutaties te realiseren tussen DGP&V/Nationale Politie en NCTV voor de financiering hiervan, mocht dat nodig zijn. Het is de verwachting dat niet de totale kosten van de competente autoriteit uit de IRU kunnen worden gefinancierd. Hiervoor zullen alternatieve financieringsmogelijkheden worden verkend.

Gezien de overeenkomsten bij het bestrijden van kinderporno en terroristische content online is door DRC en de NCTV de ambitie uitgesproken samen optrekken met als stip op de horizon één bestuursrechtelijke autoriteit die de online aanpak van zowel kinderporno als terroristische content regelt. Met het oog hierop zullen DRC en de NCTV in de zomer de mogelijkheden verkennen voor

de aanstelling van één gezamenlijke kwartiermaker, die ook een brug moet slaan tussen de business case KiPo en de – nog uit te werken –business case TCO. Notie is dat rekening wordt gehouden met van elkaar afwijkende tijdpaden (faseverschil in realisatie). Het betreft twee op zichzelf staande wets-/beleidstrajecten.

10.2e

Van: [redacted]
Aan: [redacted]
Cc: [redacted]
Onderwerp: RE: Verzoek: delen kader IRU
Datum: dinsdag 29 september 2020 14:41:27
Bijlagen: image001.jpg

10.2e Hoi [redacted],

Voor het kader is indertijd gekeken naar de NTD procedure (art. 54a Sr en art. 125p Sv). Deze bevoegdheid is beperkt tot strafbare feiten waarop tenminste 4 jaar gevangenisstraf is gesteld (art. 67 Sv feiten). In aansluiting hierop is de NTA beperkt tot de (uitings)delicten waarop tenminste 4 jaar gevangenisstraf is gesteld. Het gaat dan om opruiing en werven voor de gewapende strijd. Voor de vraag wanneer content past binnen de voorwaarden die gelden voor deze delicten is vooral gekeken naar de (toen) voorhanden zijnde jurisprudentie.

10.2.G & 10.2c Veel criteria zijn ontleend aan [redacted] zaak. Concreet worden de volgende criteria gehanteerd:

[redacted]

10.2.G en 10.2c

[redacted]

Wanneer de politie melding maakt van de aanwezigheid van content die aan de criteria voldoet, verzoekt de politie de provider de betreffende content te beoordelen in het licht van de eigen gebruikersvoorwaarden.

Mvg,

10.2e [redacted]

Van: [redacted]
Verzonden: dinsdag 29 september 2020 13:10
10.2e **Aan:** [redacted]
CC: [redacted]
Onderwerp: Verzoek: delen kader IRU

10.2e Goedemiddag [redacted],

Onze minister spreekt volgende week met BZK rondom het oprichten van een ZBO. Hiervoor stellen wij een annotatie op. Een onderdeel van deze annotatie is de bredere aanpak tegen online CT content. Daarom hebben wij aan onze juridische

10.2e afdeling [redacted] gevraagd uiteen te zetten wat de stafrechtelijke aanpak voor CT content omvat. Hiervoor hebben zij het kader nodig die de IRU in gezamenlijkheid met het OM heeft opgesteld. Het gaat hier om het kader waaraan content moet voldoen om een referral over te versturen.

Zou jij dit kader met ons kunnen delen? Ik kan mij herinneren dat jij aangaf dat dit kader nooit is herzien, maar dat is niet erg. Het kader wordt ook niet één op één gedeeld met de minister.

Ik hoor graag van je!

Met hartelijke groet,

10.2e [redacted]

Ministerie van Justitie en Veiligheid
Nationaal Coördinator Terrorismebestrijding en Veiligheid

10.2e 

Directie Contraterrorisme
T [redacted]
E [redacted]
www.nctv.nl

Van: [redacted]
Aan: [redacted]
10.2e **Cc:** [redacted]
Onderwerp: RE: Verzoek: delen kader IRU
Datum: dinsdag 29 september 2020 16:54:58
Bijlagen: image001.jpg

10.2e Hi [redacted],
[redacted] en ik hebben snel een concepttekst in elkaar gezet, maar willen graag even bij jullie toetsen of jullie dit voor ogen hadden. Zie onder. Hoor graag!
Groet,
10.2e [redacted]

Vooropgesteld: de strafrechtelijke aanpak van (extremistische) uitingen is gericht op vervolging en bestraffing van een (natuurlijk) persoon en heeft niet (zoals de TCO verordening) tot doel het tegengaan van verspreiding van terroristische inhoud. Wanneer het gaat om uitingen die aanzetten tot haat, opruien tot het plegen van strafbare feiten, werven voor de gewapende strijd of waarmee personen worden bedreigd of beledigd is het mogelijk om strafrechtelijk te vervolgen. Bij de beoordeling speelt het spanningsveld tussen de strafbaarstelling van extremistische boodschappen enerzijds en de vrijheid van meningsuiting anderzijds een belangrijke rol. Het recht op vrijheid van meningsuiting houdt op daar waar uitingen de inhoud aannemen van belediging, werven voor de gewapende strijd, aanzetten tot haat, opruiing of bedreiging.

Vervolging van (extremistische) uitingen

- In het kader van de beoordeling van extremistische uitingen zijn de belangrijkste strafbepalingen die inzake groepsbelediging (artikel 137c Sr), aanzetten tot haat, discriminatie of geweld (artikel 137d Sr), opruiing (artikelen 131 en 132 Sr), werven voor de gewapende strijd (artikel 205 Sr), eenvoudige belediging (artikel 266 Sr) en bedreiging (artikel 285 Sr). Bij beoordeling van de strafbaarheid van uitingen, wordt onderzocht of een uiting valt onder de delictsomschrijvingen van de genoemde misdrijven.
- Bij de beoordeling van uitingsdelicten speelt de context een belangrijke rol. Zo heeft de Hoge Raad bepaald dat de strafbaarheid van uitingen afhankelijk is van de aard van de uitlatingen, de eventuele onderlinge samenhang tussen verschillende uitingen en de context waarin de uitlatingen zijn gedaan (Hoge Raad 22 december 2009, NJ 2010/671).
- De context van de uiting is nog in een ander opzicht van (groot) belang bij de beoordeling van de strafbaarheid van uitingsdelicten. Bij de bepaling van de strafbaarheid van (groeps)belediging en het aanzetten tot haat dient te worden bekeken of met uitingen die in beginsel onder de delictsomschrijving vallen, een deelname aan het publieke debat is beoogd die in verband met het recht op vrijheid van meningsuiting bescherming verdient.

Verwijderen online content

- De aanpak die de NL IRU hanteert, is gebaseerd op de methode Notice and Take Action (NTA): het identificeren, duiden en melden van bepaalde content aan internetbedrijven, met het oog op verwijdering. De werkwijze van de IRU is beperkt tot strafbare feiten waarop tenminste 4 jaar gevangenisstraf is gesteld (art. 67 Sv feiten). Hieronder vallen de uitingsdelicten opruiing en werven voor de gewapende strijd. Voor de vraag wanneer (jihadistische) content past binnen de voorwaarden die gelden voor deze delicten is vooral gekeken naar jurisprudentie ontleend aan de Context zaak.
- Wanneer de NL IRU melding maakt van de aanwezigheid van content die aan de criteria voldoet, verzoekt de NL IRU de provider de betreffende content te beoordelen in het licht van de eigen gebruikersvoorwaarden.
- In die gevallen waarin de NTA-gedragscode niet afdoende is voor de verwijdering van de gegevens, bijvoorbeeld omdat verschil van inzicht bestaat over de strafbaarheid daarvan, of wanneer sprake is van een aanbieder die de gedragscode niet heeft ondertekend, kan de officier van justitie gebruikmaken van de bevoegdheid in art. 125p Sv.
- Art. 125p Wetboek van Strafrecht voorziet in de bevoegdheid een aanbieder van een communicatiedienst te bevelen gegevens, aangetroffen tijdens het

onderzoek in een geautomatiseerd werk, met betrekking tot welke of met behulp waarvan het strafbare feit is gepleegd, ontoegankelijk te maken. Hiermee wordt bereikt dat een strafbaar feit wordt beëindigd of een nieuw strafbaar feit voorkomen. Het bevel tot ontoegankelijkmaking van gegevens is beperkt tot gevallen waarin sprake is van verdenking van een misdrijf waarvoor voorlopige hechtenis mogelijk is.

- Deze bevoegdheid kan dus slechts gebruikt worden op gegevens die bij een doorzoeking in een geautomatiseerd werk worden aangetroffen. Bovendien moet tussen de gegevens en een strafbaar feit een bepaald verband bestaan, te weten: het moeten gegevens zijn met betrekking tot welke of met behulp waarvan het strafbare feit is gepleegd.

10.2e **Van:** [redacted]
Verzonden: dinsdag 29 september 2020 13:10
Aan: [redacted]
10.2e **CC:** [redacted]
Onderwerp: Verzoek: delen kader IRU

10.2e **Goedemiddag [redacted],**
Onze minister spreekt volgende week met BZK rondom het oprichten van een ZBO. Hiervoor stellen wij een annotatie op. Een onderdeel van deze annotatie is de bredere aanpak tegen
10.2e **online CT content. Daarom hebben wij aan onze juridische afdeling [redacted]**
10.2e **[redacted], in CC) gevraagd uiteen te zetten wat de stafrechtelijke aanpak voor CT content omvat. Hiervoor hebben zij het kader nodig die de IRU in gezamenlijkheid met het OM heeft opgesteld. Het gaat hier om het kader waaraan content moet voldoen om een referral over te versturen. Zou jij dit kader met ons kunnen delen? Ik kan mij herinneren dat jij aangaf dat dit kader nooit is herzien, maar dat is niet erg. Het kader wordt ook niet één op één gedeeld met de minister. Ik hoor graag van je!**

Met hartelijke groet,



10.2e
[redacted]
Ministerie van Justitie en Veiligheid
Nationaal Coördinator Terrorismebestrijding en Veiligheid
Directie Contraterrorisme
T [redacted]
E [redacted]
www.nctv.nl



Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

Directie Risico's en Dreigingen
NCTV

Contactpersoon
[redacted]

10.2e

verslag

Bespreken opties voor online 1-op-1 interventies op radicalisering aan de hand van social media analyse

Datum
29 augustus 2017

Projectnaam
-

Ons kenmerk
-

Notulist
[redacted]

10.2e

Omschrijving	Bespreken opties en juridische mogelijkheden voor online 1-op-1 interventies op radicalisering aan de hand van social media analyse
Vergaderdatum en -tijd	28 augustus 2017, 9.30 uur
Vergaderplaats	Driebergen
Aanwezig	[redacted] CTER Landelijke Eenheid politie [redacted] Internet Referral unit (IRU) [redacted] NCTV [redacted] NCTV

10.2e

De Internet Referral Unit (IRU), maatregel 29 uit het Actieprogramma, is de afgelopen maanden in proeftijd gestart en heeft als doel om bepaalde (jihadistische, terroristische) content te identificeren, duiden en melden aan internetbedrijven, met het oog op verwijdering. Tot de werkwijze behoort ook het afstemmen van meldingen en het delen van content met relevante partners binnen en buiten de politie, waaronder de EU IRU van Europol. De IRU gaat officieel 1 september van start, momenteel wordt personeel geworven.

Goed nieuws is dat de IRU [redacted] content verwijdert, [redacted]

10.2.C & 10.2.G

V.w.b. content heeft de IRU 3 routes:

- [redacted]

11.1

De IRU en CTER zien zeker meerwaarde in ons idee van online 1-op-1 interventies. Toepassingen die zij zien:

10.2.C en 10.2.G. • [redacted]

11.1 • [redacted]

11.1 [redacted]

11.1 [redacted]

Politie ziet het als een goede rol voor de NCTV om de online aanpak te stimuleren, structureren en aanspreekpunt voor te zijn.

We hebben afgesproken dat we contact houden over de voortgang en dat de IRU over enkele maanden [redacted]

10.2.C & 10.2.G [redacted]

Openstaande vragen:

11.1 - [redacted]

- wanneer is er sprake van een referral en wanneer van een strafrechtelijk onderzoek?

11.1 - [redacted]